Reduction modulo p of two-dimensional crystalline representations of $G_{\mathbb{Q}_p}$ of slope less than three

Bodan Arsovski†

May, 2015

Abstract. We use the p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ to find the reduction modulo p of certain two-dimensional crystalline Galois representations, following the approach used in [14] and [15]. In particular, we resolve a conjecture of Breuil, Buzzard, and Emerton in the case when the slope is strictly between one and three, and prove partial results towards this conjecture for arbitrary slopes. Moreover, we partially classify the reduction modulo p of these representations when the slope is equal to one.

Keywords. *crystalline representations, local Langlands correspondence, modular forms.*

†Department of Mathematics, Imperial College London, 180 Queen's Gate, London SW7 2AZ, United Kingdom

Contents

1 Introduction

1.1 Definitions and notation

Throughout this paper, we assume that $p>2$ is an odd prime number, we let $K=\mathrm{GL}_2(\mathbb{Z}_p)$, and we let Z be the centre of $G=\mathrm{GL}_2(\mathbb{Q}_p)$. If R is a $\mathbb{Z}_p$-algebra, we define $\mathrm{Symm}^r(R)$ to be the space of homogeneous polynomials in $R[x,y]$ which have degree r. There is the obvious right action of K on $\mathrm{Symm}^r(R)$, which is defined in section 2 of [14], and which can be extended to an action of KZ by letting pI act trivially. We let $I(V)$ be the compact induction $\mathrm{ind}_{KZ}^G(V)$—the space of functions $f:G\to V$ which have compact support modulo Z and which satisfy $f(\kappa g)=\kappa f(g)$ for all $\kappa\in KZ$. There is a right action of G on $I(V)$ defined by $fg(\gamma)=f(\gamma g)$. If $V=\mathrm{Symm}^r(R^2)$

then there is an endomorphism T of $I(V)$ which corresponds to the function $G \to \mathrm{End}_R(V)$ which is supported on $KZ\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)KZ$ and sends $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to the map $\psi(x,y) \mapsto \psi(px,y)$. We let $[g,v]$ be the unique element of $I(V)$ which is supported on KZg^{-1} and which satisfies $[g,v]g^{-1} = v$. Then $g[h,v] = [gh,v]$ for $g,h \in G$, and $[g\kappa,v] = [g,v\kappa]$ for $\kappa \in KZ$, and the $[g,v]$ span $I(V)$ as an abelian group. In section 2 of [9] it is shown that T can be written as

$$T[g,v] = \textstyle\sum_{\lambda \in \mathbb{F}_p} [g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), v(x, -[\lambda]x + py)] + [g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), v(px,y)] \,.$$

Here $[\lambda]$ is the Teichmüller lift of λ to $\mathbb{Z}_p$. The same equation defines an endomorphism T of $I(\det^s \otimes \mathrm{Symm}^r(\overline{\mathbb{F}}_p^2))$. We denote $\mathrm{Symm}^r(\overline{\mathbb{F}}_p^2)$ by σ_r. We denote by $\sigma_m(n)$ the twist $\det^n \otimes \sigma_m$. We denote by ω the $\bmod p$ reduction of the cyclotomic character, and we denote by ω_2 the $\bmod p$ reduction of a choice of a fundamental character of niveau 2. If $\chi : \mathbb{Q}_p^\times \to \overline{\mathbb{F}}_p^\times$ is a character, if $\lambda \in \overline{\mathbb{F}}_p$, and if $0 \leqslant \nu \leqslant p-1$, then we define $\pi(\nu,\lambda,\chi) = (\chi \circ \det) \otimes (I(\sigma_\nu)/(T-\lambda))$. If R is a ring and $t \in R^\times$, then we let μ_t denote the map $\mathrm{GL}_1(\mathbb{Q}_p) \to R^\times$ which is trivial on $\mathbb{Z}_p^\times$ and which sends p to t. The following classification of the modules $\pi(\nu,\lambda,\chi)$ is given in sections 2 and 3 of [14].

Theorem 1. *1. If $(\nu,\lambda) \notin \{(0,\pm1),(p-1,\pm1)\}$, then $\pi(\nu,\lambda,\chi)$ is irreducible. The modules $\pi(\nu,\lambda,\chi)$ with $\lambda = 0$ are the supersingular representations of G; no Jordan–Hölder factor of $\pi(\nu,\lambda,\chi)$ with $\lambda \neq 0$ is supersingular.*

2. *Each $\pi(\nu,\lambda,\chi)$ has finite length.*

3. *The only isomorphisms between the $\pi(\nu,\lambda,\chi)$ are the following:*

   — *if $\lambda \neq 0$ and $(\nu,\lambda) \notin \{(0,\pm1),(p-1,\pm1)\}$, then $\pi(\nu,\lambda,\chi) \cong \pi(\nu,-\lambda,\chi\mu_{-1})$;*

   — *if $\lambda \notin \{0,\pm1\}$, then $\pi(0,\lambda,\chi) \cong \pi(p-1,-\lambda,\chi)$;*

   — *$\pi(\nu,0,\chi) \cong \pi(\nu,0,\chi\mu_{-1}) \cong \pi(p-1-\nu,0,\chi\omega^\nu) \cong \pi(p-1-\nu,0,\chi\omega^\nu\mu_{-1})$.*

4. *If $\lambda \neq 0$, and if $\pi(\nu,\lambda,\chi)$ and $\pi(\nu',\lambda',\chi')$ have a common Jordan–Hölder factor, then $\lambda' \neq 0$, $\nu \equiv_{p-1} \nu'$, and χ/χ' is unramified.*

5. *If $0 \leqslant \nu \leqslant p-1$, and if F is a quotient of $I(\det^l \otimes \sigma_\nu)$ which has finite length as an $\overline{\mathbb{F}}_p[G]$-module, then every Jordan–Hölder factor of F is a subquotient of $\pi(\nu,\lambda,\omega^l)$, for some λ which possibly depends on the factor.*

If $f = \sum_{n \geqslant 1} a_n q^n$ is an eigenform for the subgroup $\Gamma_1(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$, which has character ψ, then there is a p-adic Galois representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p).$$

If $\ell \neq p$ is a prime distinct from p, then the local structure at ℓ of the Galois representation ρ_f associated with f can be explicitly described. The local structure at p of ρ_f is in general more complicated. However, the reduction $\overline{\rho}_f|_{D_p}$ modulo p can be classified; if $\overline{\rho}_f|_{D_p}$ is reducible then its semisimplifaction is the sum of two characters, and if $\overline{\rho}_f|_{D_p}$ is irreducible then it is induced from characters of the absolute Galois group of the unramified quadratic extension of $\mathbb{Q}_p$. When N and p are coprime, then $\overline{\rho}_f|_{D_p}$ can be determined from the weight k, the coefficient $a_p = a$ of the q-series expansion, and the character ψ. If $r \geqslant 0$, then there is a uniquely determined two-dimensional crystalline representation $V_{r+2,a}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ which has Hodge–Tate weights 0 and $r+1$, determinant the cyclotomic character to the power of $r+1$, and $X^2 - aX + p^{r+1}$ as the characteristic polynomial of crystalline Frobenius on the contravariant Dieudonne module. A construction of this representation is given for example in [9]. This is the local Galois representation at p associated with the eigenform $f = \sum_{n \geqslant 1} a_n q^n$ of weight $k = r+2$. We will denote by $\overline{V}_{r+2,a}$ the semisimplification of the reduction of $V_{r+2,a}$ modulo the maximal ideal of $\overline{\mathbb{Z}}_p$. If $r \geqslant 0$, and $a \in \overline{\mathbb{Q}}_p$ is such that $v(a) > 0$, and if the roots of $X^2 - aX + p^{r+1}$ do

not have ratio $p^{\pm 1}$ or 1, then we define

$$\Pi_{r+2,a} = I(\mathrm{Symm}^r(\overline{\mathbb{Q}}_p^2))/(T-a),$$

and we let $\Theta_{r+2,a}$ be the image of $I(\mathrm{Symm}^r(\overline{\mathbb{Z}}_p^2))$ in $\Pi_{r+2,a}$. There is a natural surjective map

$$I(\sigma_r) \twoheadrightarrow \overline{\Theta}_{r+2,a} = \Theta_{r+2,a} \otimes \overline{\mathbb{F}}_p.$$

The following theorem is the p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$, and is given, for example, in section 1 of [9] and in section 2 of [14].

Theorem 2. *If the roots of $X^2 - aX + p^{r+1}$ do not have ratio 1 or $p^{\pm 1}$, then*

$$\begin{aligned}
&\overline{V}_{r+2,a} \cong (\mathrm{ind}(\omega_2^{\nu+1})) \otimes \chi \\
&\qquad \iff \quad (\overline{\Theta}_{r+2,a})^{\mathrm{ss}} \cong \pi(\nu, 0, \chi); \\
&\overline{V}_{r+2,a} \cong (\mu_\lambda \omega^{\nu+1} \oplus \mu_{\lambda^{-1}}) \otimes \chi \\
&\qquad \iff \quad (\overline{\Theta}_{r+2,a})^{\mathrm{ss}} \cong \pi(\nu, \lambda, \chi)^{\mathrm{ss}} \oplus \pi((p-3-\nu) \bmod (p-1), \lambda^{-1}, \chi\omega^{\nu+1})^{\mathrm{ss}}.
\end{aligned}$$

If N and p are not coprime, say $N = N'p^m$ with $\gcd(N', p) = 1$, and if the p-part χ of the character ψ has conductor p^m, then again the reduction $\overline{\rho}_f|_{D_p}$ can be determined from the weight k, the p^{th} coefficient of the q-series expansion, and the character ψ. We will denote by $\overline{V}_{r+2,a,\chi}$ the semisimplification of this reduction modulo the maximal ideal of $\overline{\mathbb{Z}}_p$.

1.2 Statements of the main results

1.2.1 In the interior of the weight space

Theorem 3.2.1 in [3], theorem 1.6 in [14], and corollary 4.7 in [15] completely determine $\overline{V}_{r+2,a}$ in the following cases (with $p > 2$):

1. $0 \leqslant r \leqslant 2p-1$;
2. $r > 2p-1$ and $v(a) < 1$;
3. $r > 2p-1$ and $v(a) > \lfloor \frac{r}{p-1} \rfloor$.

In this paper we are concerned with the remaining case: when $r \geqslant 2p$ and $\lfloor \frac{r}{p-1} \rfloor \geqslant v(a) \geqslant 1$. The papers [13] and [16] give surveys of the known results and conjectures about p-adic slopes of modular forms. In particular, the following conjecture is given in section 4 of [16].

Conjecture 3 (Breuil, Buzzard, Emerton)**.** *If r is even and $v(a) \notin \mathbb{Z}$, then $\overline{V}_{r+2,a}$ is irreducible.*

We prove partial results towards this conjecture, in addition to giving a partial classification of $\overline{V}_{r+2,a}$ in the case when $v(a) = 1$. Let r be a positive integer such that $r = t(p-1) + s$, with $t \geqslant 0$ and $s \in \{1, \ldots, p-1\}$. Let $a \in \overline{\mathbb{Q}}_p$ will be such that and $v(a) \geqslant 1$, and such that the roots of $X^2 - aX + p^{r+1}$ do not have ratio 1 or $p^{\pm 1}$. In particular, due to a theorem on Newton polygons, the second condition will always hold true whenever $r > 2v(a)$. We will interchangeably refer to the coefficient a_p by a, and to the valuation $v(a)$ by v. In section 4, we give a partial classification of $\overline{V}_{r+2,a}$ in the case when $v(a) = 1$. More specifically, we show the following theorem.

Theorem 4. *Let $v = 1$, and $s \notin \{1, 3\}$.*

1. *If $p \nmid r - s$, then $\overline{V}_{r+2,a}$ is one of $\{\mu_\lambda \omega^s \oplus \mu_{\lambda^{-1}}\omega, \mathrm{ind}(\omega_2^{s+p})\}$, where $\lambda = \overline{a/p} \cdot \frac{s}{s-r}$.*
2. *If $p \mid r - s$, then $\overline{V}_{r+2,a}$ is one of $\{\mathrm{ind}(\omega_2^{s+1}), \mathrm{ind}(\omega_2^{s+p})\}$.*

In section 5, we prove special cases of conjecture 3, when the slope is small. More specifically, we show the following theorems.

Theorem 5. *If r is even and $2 > v > 1$, then $\overline{V}_{r+2,a}$ is irreducible.*

Theorem 6. *If r is even and $3 > v > 2$, then $\overline{V}_{r+2,a}$ is irreducible.*

Theorem 7. *Let $4 > v > 3$ and let r be even. Then $\overline{V}_{r+2,a}$ is irreducible whenever*

$$r \not\equiv \{3p+1, 3p+3, 4p, 4p+2, 5p+1, 6p, s, s+p-1, s+2p-2\} \pmod{p(p-1)}.$$

Let $x^{(n)} = x(x+1)\cdots(x+n-1)$ denote the rising factorial power.

Conjecture 8. *If r is even and $v \notin \mathbb{Z}$, then $\overline{V}_{r+2,a}$ is irreducible in the following cases.*

1. If $s \in \{2, \ldots, 2\lfloor v \rfloor\}$, and if the extra condition $p \nmid (r-s)^{(2\lfloor v \rfloor+1)}$ holds true.

2. If $s \notin \{2, \ldots, 2\lfloor v \rfloor\}$, and if the extra condition $p \nmid (r-s)^{(\lfloor v \rfloor)}$ holds true. In fact, in this case

$$\overline{V}_{r+2,a} \cong \mathrm{ind}(\omega_2^{s+(p-1)\lfloor v \rfloor+1}).$$

3. If $s \notin \{2, \ldots, 2\lfloor v \rfloor\}$.

Theorem 9. *We have the following partial results towards conjecture 8.*

1. The first part of conjecture 8 is true when $6 > v$.

2. The second part of conjecture 8 is true when $38 > v$.

3. The third part of conjecture 8 is true when $3 > v$.

By combining these theorems with previously known results about conjecture 3 (for $v > \lfloor \frac{r}{p-1} \rfloor$), we can deduce the following corollary.

Corollary 10. *Conjecture 3 is true in the following cases:*

* $3 > v > 1$;
* $4 > v > 3$, *and*

$$r \not\equiv \{3p+1, 3p+3, 4p, 4p+2, 5p+1, 6p, s, s+p-1, s+2p-2\} \pmod{p(p-1)};$$

* $6 > v$, *and* $s \in \{2, \ldots, 2\lfloor v \rfloor\}$, *and* $p \nmid (r-s)^{(2\lfloor v \rfloor+1)}$;
* $38 > v$, *and* $s \notin \{2, \ldots, 2\lfloor v \rfloor\}$, *and* $p \nmid (r-s)^{(\lfloor v \rfloor)}$.

In particular, Conjecture 3 is true when $6 > v$ and $p \nmid (r-s)^{(2\lfloor v \rfloor+1)}$.

1.2.2 Near the boundary of the weight space

No local results are known when $N = N'p^m$ with $\gcd(N', p) = 1$ and $m > 0$, though a result similar to conjecture 3 is expected to hold true when the p-part of the character has conductor p^m. In particular, the following conjecture is given in section 4 of [16] (the full statement of conjecture 4.2.1 in [16] includes the case when $p = 2$, but in this paper we are only interested in the case when p is odd).

Conjecture 11 (Buzzard, Gee)**.** *If $m \geqslant 2$ and $(p-1)p^{m-2}v(a) \notin \mathbb{Z}$, then $\overline{V}_{r+2,a,\chi}$ is irreducible.*

There are global results, in [17, 22, 19, 20], which show that $(p-1)p^{m-2-\delta_{p=2}}v(\alpha) \in \mathbb{Z}$ when α is an eigenvalue of U_p on a space of modular forms of level $2^m, 3^m, 5^2, 7^2$, respectively. More results close to the boundary of weight space are proven in [22, 24].

1.3 Assumptions

In the remainder of this paper, we will make the following assumptions:

— r will be a positive integer such that $r = t(p-1)+s$, with $t \geqslant 0$ and $s \in \{1,\dots,p-1\}$;

— $a \in \overline{\mathbb{Q}}_p$ will be such that and $v(a) \geqslant 1$, and such that the roots of $X^2 - aX + p^{r+1}$ do not have ratio $p^{\pm 1}$ or 1. The second condition will always hold true whenever $r > 2v(a)$.

2 Auxiliary lemmas

2.1 Properties of the maps Ψ_α

We define the map $\Psi : \sigma_r \to \sigma_{p-1-s}(s)$ as follows:

$$\begin{aligned}\Psi : \sigma_r &\to \sigma_{p-1-s}(s)\\ f &\mapsto \textstyle\sum_{u,v\in\mathbb{F}_p} f(u,v)(vX-uY)^{p-1-s}.\end{aligned}$$

It can be shown that this map is surjective and $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant, and it induces a map on the induction $I(\sigma_r)$. We will denote this induced map also by Ψ.

Lemma 12. *Let $t \geqslant 2$ be an integer, and suppose that $r = t(p-1)+s$, with $s \in \{1,\dots,p-1\}$. Suppose moreover that $l \in \{1,\dots,t\}$ and $i \in \{0,\dots,s-1\}$. Then $\Psi x^{r-i}y^i = \Psi x^i y^{r-i} = 0$, and $\Psi x^{l(p-1)}y^{r-l(p-1)} = X^{p-1-s}$.*

Proof. If $0 \leqslant i \leqslant r$, then

$$\begin{aligned}[X^jY^{p-j-1-s}]\Psi x^i y^{r-i} &= \textstyle\sum_{u,v\in\mathbb{F}_p} (-1)^{j+s}\binom{p-1-s}{j} u^{i+p-j-1-s} v^{r-i+j}\\ &= (-1)^{j+s}\binom{p-1-s}{j} \textstyle\sum_{u\in\mathbb{F}_p} u^{i+p-j-1-s} \sum_{v\in\mathbb{F}_p} v^{r-i+j}\\ &= (-1)^{j+s}\binom{p-1-s}{j}\,\Xi_{i,j},\end{aligned}$$

where for convenience we use the notation $0^0 = 1$. This implies that $\sum_{u\in\mathbb{F}_p} u^\xi = \delta_{\xi\equiv_{p-1}0}\delta_{\xi\neq 0}$, where $\delta_P = 1$ if P holds true and $\delta_P = 0$ otherwise. Then

$$\begin{aligned}\Xi_{ij} &= \delta_{i+p-j-1-s\equiv_{p-1}0}\delta_{i+p-j-1-s\neq 0}\delta_{r-i+j\equiv_{p-1}0}\delta_{r-i+j\neq 0}\\ &= \delta_{j\equiv_{p-1}i-s}\delta_{(i,j)\notin\{(0,p-1-s),(r,0)\}}\\ &= \delta_{j\equiv_{p-1}i-s}\delta_{i\notin\{0,r\}}.\end{aligned}$$

Consequently,

$$[X^jY^{p-j-1-s}]\Psi x^i y^{r-i} = (-1)^{j+s}\binom{p-1-s}{j}\delta_{j\equiv_{p-1}i-s}\delta_{i\notin\{0,r\}}.$$

Since $j \in \{0,\dots,p-1-s\}$, then $\delta_{j\equiv_{p-1}i-s}\delta_{i\notin\{0,r\}} = 0$ whenever $i \in \{0,\dots,s-1\}$, so $\Psi x^i y^{r-i} = 0$. Since Ψ is $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant, then $\Psi x^{r-i}y^i = 0$ whenever $i \in \{0,\dots,s-1\}$ as well. Finally, if $l \in \{1,\dots,t\}$, then

$$\Psi x^{l(p-1)}y^{r-l(p-1)} = (-1)^{p-1}\binom{p-1-s}{p-1-s}X^{p-1-s} = X^{p-1-s},$$

which completes the proof. $\square$

Lemma 13. *Let $t \geqslant 1$ be an integer, and suppose that $r = t(p-1)+s$, with $s \in \{1,\dots,p-1\}$. In $I(\sigma_{p-1-s}(s))$,*

$$T : [1, X^{p-1-s}] \mapsto \textstyle\sum_{\mu\in\mathbb{F}_p}\left[\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right), X^{p-1-s}\right] + \delta_{s=p-1}\left[\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), X^{p-1-s}\right],$$

where $\delta_{s=p-1} = 1$ *if* $s = p-1$, *and* $\delta_{s=p-1} = 0$ *otherwise.*

Proof. Immediate from the definition of T. $\square$

Let $h \geqslant 0$ be an integer, and suppose that $r \geqslant h(p+1)$. We define the map

$$\begin{aligned} \Psi_h : \overline{\theta}^h \sigma_{r-h(p+1)} \subseteq \sigma_r &\to \sigma_{(2h-r \bmod p-1)}(r-h) \\ \overline{\theta}^h f &\mapsto \overline{\theta}^h \Psi f. \end{aligned}$$

This map is surjective and $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant, due to the fact that $\overline{\theta}^h \sigma_{r-h(p+1)} \cong \sigma_{r-h(p+1)}(h)$, and it induces a map on $I(\overline{\theta}^h \sigma_{r-h(p+1)})$. We will denote this induced map also by Ψ_h.

2.2 Properties of the kernel of reduction $X(r+2,a)$

The following statement is a technical lemma about modules.

Lemma 14. *Suppose that* A, B, C *are modules and* $\beta : A \to B$ *and* $\gamma : A \to C$ *are surjective maps. Suppose that* $B' \subseteq B$ *is a submodule such that, for all* $b' \in B'$, *there exists a* $c' \in \ker\gamma$ *such that* $\beta(c') = b'$. *Then there is a series* $C = C_2 \supseteq C_1 \supseteq C_0 = \{0\}$ *of length two, whose factor* C/C_1 *is isomorphic to a quotient of* B/B' *and whose other factor* C_1 *is isomorphic to* $\ker\beta/(\ker\beta \cap \ker\gamma)$.

Proof. There is the composition map $A \xrightarrow{\gamma} C \xrightarrow{q} C/\gamma(\ker\beta)$. This map is surjective, and its kernel contains $\ker\beta$. Let $C_1 = \gamma(\ker\beta)$. Then $C_1 \cong \ker\beta/\ker(\gamma|_{\ker\beta}) = \ker\beta/(\ker\beta \cap \ker\gamma)$. Moreover, we have $\ker\gamma q = \ker\beta + \ker\gamma$. Because of the condition that, for all $b' \in B'$, there exists a $c' \in \ker\gamma$ such that $\beta(c') = b'$, we know that $\ker\beta + \ker\gamma \supseteq \ker\beta + \beta^{-1}(B')$. Hence $C/C_1 \cong A/(\ker\beta + \ker\gamma)$ is isomorphic to a quotient of $A/(\ker\beta + \beta^{-1}(B'))$, which is isomorphic to B/B' by several applications of the isomorphism theorems. $\square$

Let $X(r+2,a)$ denote the kernel of the surjection $I(\sigma_r) \twoheadrightarrow \overline{\Theta}_{r+2,a}$. The following statements can be proven by the same method used to show lemmas 4.1 and 4.3 in [14].

Lemma 15. *1. Let* $r \geqslant 2(p+1)$, *and suppose that* $a \in \overline{\mathbb{Q}}_p$ *is such that* $2 > v(a) \geqslant 1$. *Denote by* $\overline{\theta}$ *the polynomial* $xy^p - x^py \in \overline{\mathbb{F}}_p[x,y]$. *Then* $X(r+2,a)$ *contains* $I(Y_r)$, *where* Y_r *is the subrepresenation of* σ_r *generated by* $\overline{\theta}^2 \sigma_{r-2(p+1)}$ *and* y^r.

2. Let $r \geqslant (m+1)(p+1)$, *and suppose that* $a \in \overline{\mathbb{Q}}_p$ *is such that* $m+1 > v(a) > m$. *Then* $X(r+2,a)$ *contains the induction of the subrepresenation of* σ_r *generated by* $\overline{\theta}^{m+1} \sigma_{r-(m+1)(p+1)}$ *and* $\{y^r, xy^{r-1}, \ldots, x^m y^{r-m}\}$.

Before proving lemma 15, we will first show two auxiliary results.

Lemma 16. *Let* $r, m, n, c \geqslant 0$ *be integers, and let* $a \in \overline{\mathbb{Q}}_p$ *be such that* $m+1 > v(a) > m$. *Suppose that* $n \geqslant m+1$, *and* $r \geqslant np + c$. *Then there is some* $\phi_{r,m,n,c,g}$ *such that*

$$\begin{aligned} (T-a)\phi_{r,m,n,c,g} \equiv &\textstyle\sum_j (-1)^j \binom{n}{j} p^{r-j(p-1)-c} \left[g\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), x^{j(p-1)+c} y^{r-j(p-1)-c} \right] \\ &+ \textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+c} \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), x^{j(p-1)+c} y^{r-j(p-1)-c} \right] \\ &- a \textstyle\sum_j (-1)^j \binom{n-\alpha}{j} \left[g, \theta^\alpha x^{j(p-1)+c-\alpha} y^{r-\alpha p-j(p-1)-c} \right] \pmod{p^n}, \end{aligned}$$

for all $0 \leqslant \alpha \leqslant n$.

Proof. For $0 \leqslant j \leqslant n$, let $\varphi_{c,j,g} = \left[g, x^{j(p-1)+c} y^{r-j(p-1)-c}\right]$, and let $\phi^{(0)}_{n,c,g} = \sum_j (-1)^j \binom{n}{j} \varphi_{c,j,g}$. Then

$$\begin{aligned}(T-a)\phi^{(0)}_{n,c,g} &\equiv \textstyle\sum_{\lambda \neq 0} \sum_{z \geqslant 0} p^z \sum_j (-1)^j \binom{n}{j} \binom{r-j(p-1)-c}{z} \left[g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), (-[\lambda])^{r-c-z} x^{r-z} y^z\right] \\ &\quad + \textstyle\sum_j (-1)^j \binom{n}{j} p^{r-j(p-1)-c} \left[g\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \\ &\quad + \textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+c} \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \\ &\quad - a \textstyle\sum_j (-1)^j \binom{n}{j} \left[g, x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \\ &\equiv \textstyle\sum_j (-1)^j \binom{n}{j} p^{r-j(p-1)-c} \left[g\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \\ &\quad + \textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+c} \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \\ &\quad - a \textstyle\sum_j (-1)^j \binom{n}{j} \left[g, x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \pmod{p^n}.\end{aligned}$$

Note that, for all $0 \leqslant \alpha \leqslant n$,

$$\begin{aligned}&a \textstyle\sum_j (-1)^j \binom{n}{j} \left[g, x^{j(p-1)+c} y^{r-j(p-1)-c}\right] \\ &\quad = a \textstyle\sum_{u,w} (-1)^{u+w} \binom{n-\alpha}{u} \binom{\alpha}{w} \left[g, x^{(u+w)(p-1)+c} y^{r-(u+w)(p-1)-c}\right] \\ &\quad = a \textstyle\sum_u (-1)^u \binom{n-\alpha}{u} \left[g, x^{u(p-1)+c-\alpha} y^{r-\alpha p-u(p-1)-c} \sum_w \binom{\alpha}{w} x^{w(p-1)+\alpha} y^{\alpha p-w(p-1)}\right] \\ &\quad = a \textstyle\sum_u (-1)^u \binom{n-\alpha}{u} \left[g, \theta^\alpha x^{u(p-1)+c-\alpha} y^{r-\alpha p-u(p-1)-c}\right].\end{aligned}$$

Consequently, $\phi_{r,m,n,c,g} = \phi^{(0)}_{n,c,g}$ has the desired properties. ☐

Lemma 17. *Let $r, m, n, \alpha \geqslant 0$ be integers, and let $a \in \overline{\mathbb{Q}}_p$ be such that $m+1 > v(a) > m$. Suppose that $n \geqslant m+1$, and $n \geqslant \alpha$, and $r \geqslant np+\alpha$. Then there are some $\phi^*_{r,m,n,\alpha,g}$ and $\phi^{**}_{r,m,n,\alpha,g}$ such that*

$$\begin{aligned}(T-a)\phi^*_{r,m,n,\alpha,g} &\equiv \textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+\alpha} \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha}\right] \\ &\quad - a \textstyle\sum_j (-1)^j \binom{n-\alpha}{j} \left[g, \theta^\alpha x^{j(p-1)} y^{r-\alpha(p+1)-j(p-1)}\right] \pmod{p^n},\end{aligned}$$

and

$$\begin{aligned}(T-a)\phi^{**}_{r,m,n,\alpha,g} &\equiv \textstyle\sum_j (-1)^j \binom{n}{j} p^{j(p-1)+\alpha} \left[g\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right), y^{j(p-1)+\alpha} x^{r-j(p-1)-\alpha}\right] \\ &\quad - (-1)^\alpha a \textstyle\sum_j (-1)^j \binom{n-\alpha}{j} \left[g, \theta^\alpha y^{j(p-1)} x^{r-\alpha(p+1)-j(p-1)}\right] \pmod{p^n}.\end{aligned}$$

Proof. Take $\phi^*_{r,m,n,\alpha,g} = \phi_{r,m,n,\alpha,g}$ and $\phi^{**}_{r,m,n,\alpha,g} = \phi_{r,m,n,\alpha,g\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)}$. ☐

Proof of lemma 15. First, we will show that if $r, m \geqslant 0$ are such that $r \geqslant (m+1)(n+1)$, and if $m+1 > v(a) \geqslant m$, then $X(r+2,a)$ contains the induction of $\overline{\theta}^{m+1} \sigma_{r-(m+1)(p+1)}$. Then, we will show that if $r, m \geqslant 0$ are such that $r \geqslant (m+1)(n+1)$, and if $m+1 \geqslant v(a) > m$, then $X(r+2,a)$ contains the induction of the subrepresentation of σ_r generated by $\{y^r, xy^{r-1}, \ldots, x^m y^{r-m}\}$. These two results will imply the two claims stated in lemma 15. For the first part, note that, for any $f \in \overline{\mathbb{Z}}_p[x,y]$ of degree $r-(m+1)(p+1)$, we have $[1, \theta^{m+1} f] = \sum_j \lambda_j \phi^{(0)}_{m+1,c_j,1}$ for some λ_j and some $r-m-1 \geqslant c_j \geqslant m+1$, so

$$(T-a)\left[1, \theta^{m+1} f\right] = (T-a) \textstyle\sum_j \lambda_j \phi^{(0)}_{m+1,c_j,1} \equiv -a \left[1, \theta^{m+1} f\right] \pmod{p^{m+1}}.$$

Consequently, $\overline{(T-a)\left[1, -a^{-1} \theta^{m+1} f\right]} = \left[1, \overline{\theta}^{m+1} f\right]$ is in the kernel of reduction. For the second part, note that, for $0 \leqslant \alpha \leqslant m$,

$$(T-a)\left(p^{-\alpha} \phi^*_{r,m,m+1,\alpha,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)}\right) \equiv [1, x^\alpha y^{r-\alpha}] \pmod{p^{v(a)-m}}.$$

Consequently, $[1, x^\alpha y^{r-\alpha}]$ is in the kernel of reduction, for all $0 \leqslant \alpha \leqslant m$. $\square$

The subrepresentation $\ker \Psi$ is isomorphic to W_r, where W_r is the subrepresentation of σ_r generated by $\overline{\theta}\sigma_{r-(p+1)}$ and $\{y^r, xy^{r-1}, \ldots, x^{s-1}y^{r-s+1}\}$. We showed this in the proof of lemma 12, where we stated an explicit matrix representation of Ψ. In fact, W_r is generated by $\overline{\theta}\sigma_{r-(p+1)}$ and y^r only; indeed, $W_r' = \langle \overline{\theta}\sigma_{r-(p+1)}, y^r \rangle_K \subseteq W_r$, and $\sigma_r / W_r \cong \sigma_{p-1-s}$ since Ψ is surjective, and also $\sigma_r / W_r' \cong \sigma_{p-1-s}(s)$ due to corollary 5.1 in [14]. Consequently,

$$I(\ker \Psi) = I\left(\langle \overline{\theta}\sigma_{r-(p+1)}, y^r \rangle_{\mathrm{GL}_2(\mathbb{F}_p)}\right).$$

The following lemma gives a linear basis for $\langle y^r, xy^{r-1}, \ldots, x^m y^{r-m} \rangle_{\mathrm{GL}_2(\mathbb{F}_p)} \subseteq \sigma_r$.

Lemma 18. *Let $r \geqslant (m+1)(p+1)$, and let $p > m+1$. Then the subrepresentation S_m of σ_r generated by $\{y^r, xy^{r-1}, \ldots, x^m y^{r-m}\}$ is linearly spanned by*

$$\begin{aligned} &\{y^r, xy^{r-1}, \ldots, x^m y^{r-m}\} \cup \{x^r, x^{r-1}y \ldots, x^{r-m}y^m\} \\ &\quad \cup \left\{ \textstyle\sum_{r-m > s(p-1)+i > m} \binom{r-m}{s(p-1)+j} x^{s(p-1)+i} y^{r-s(p-1)-i} \,\middle|\, i, j \in \mathbb{Z} \text{ with } i-j \in \{0, \ldots, m\} \right\} \\ &\quad \cup \left\{ \textstyle\sum_{r-m > s(p-1)+i > m} \binom{r-m}{s(p-1)+j} y^{s(p-1)+i} x^{r-s(p-1)-i} \,\middle|\, i, j \in \mathbb{Z} \text{ with } i-j \in \{0, \ldots, m\} \right\}. \end{aligned}$$

Proof. Let S_m' denote the subrepresentation of σ_r generated by $x^m y^{r-m}$. Then S_m' is a subrepresentation of S_m. Moreover, $\sum_{\mu \in \mathbb{F}_p^\times} \lambda_\mu (x + \mu y)^m y^{r-m} = \sum_{i=0}^m \nu_i x^i y^{m-i}$ is in S_m', where

$$\nu_i = \textstyle\sum_{\mu \in \mathbb{F}_p^\times} \lambda_\mu \mu^i = \sum_{s=0}^{p-1} \lambda_s t^{is} = f(t^i),$$

where t is a generator for $\mathbb{F}_p^\times$. Since the number of ν_i is $m+1 \leqslant p-1 = \deg f$, the coefficients of f can be chosen in a way that $\nu_i = \delta_{i=\alpha}$. Consequently, $x^\alpha y^{r-\alpha}$ is in S_m', for all $0 \leqslant \alpha \leqslant m$, which implies that $S_m' = S_m$. So S_m is equal to the linear span of $(ax+cy)^m (bx+dy)^{r-m}$. Since either $ad \neq 0$ or $bc \neq 0$, then S_m is equal to the linear span of $(x+ay)^m (bx+y)^{r-m}$ and $(x+ay)^m (bx+y)^{r-m} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. By a similar argument as in the previous paragraph, the linear span of $(x+ay)^m (bx+y)^{r-m}$ is the same as the linear span of $x^i y^{m-i} (bx+y)^{r-m}$, for $i \in \{0, \ldots, m\}$ and $b \in \mathbb{F}_p$. By another application of this argument, the linear span of $x^i y^{m-i} (bx+y)^{r-m}$ is the same as the linear span of $y^r, xy^{r-1}, \ldots, x^m y^{r-m}$, and $\sum_s \binom{r-m}{s(p-1)+j} x^{s(p-1)+i} y^{r-s(p-1)-i}$, for $i, j \in \mathbb{Z}$ such that $i - j \in \{0, \ldots, m\}$. Similarly, the linear span of $(x+ay)^m (bx+y)^{r-m} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is the same as the linear span of $x^r, yx^{r-1}, \ldots, y^m x^{r-m}$, and $\sum_s \binom{r-m}{s(p-1)+j} y^{s(p-1)+i} x^{r-s(p-1)-i}$, for $i, j \in \mathbb{Z}$ such that $i - j \in \{0, \ldots, m\}$. The proof of the lemma can be completed by combining these two results. $\square$

The module I_h is defined in [1] for each integer h, as the module of $\mathbb{F}_p$-valued functions on $\mathbb{F}_p^2$ which are homogeneous of degree h and which vanish at the origin. By definition, $I_h = I_{\widetilde{h}}$, where $\widetilde{h}$ is the integer in $\{1, \ldots, p-1\}$ which is congruent to h modulo $p-1$.

Lemma 19. *Whenever $p > h > 0$ and $t \in \mathbb{Z}$, the module $I_h(t)$ is semi-simple if and only if $h = p-1$. If $p-1 > h > 0$, then the only possible quotients of $I_h(t)$ are $I_h(t), \sigma_{p-1-h}(t+h)$, and the trivial quotient. If $h = p-1$, then $I_h(t) = I_{p-1}(t) = \sigma_{p-1}(t) \oplus \sigma_0(t)$, so there is the additional possible quotient $\sigma_0(t)$.*

Proof. Due to parts (a) and (c) of lemma 3.2 in [1], $I_h(t)$ has a series

$$I_h(t) = N_2 \supseteq N_1 \supseteq N_0 = \{0\},$$

whose factors are $N_2/N_1 \cong \sigma_{p-1-h}(t+h)$ and $N_1 \cong \sigma_h(t)$. Then $I_h(t)$ is semi-simple if and only if $I_h(t) = N_1 \oplus M$, where $M \cong \sigma_{p-1-h}(t+h)$. Since M inherits the action of $I_h(t)$, this is possible only when $h = p-1$, in which case indeed $I_h(t) = I_{p-1}(t) = \sigma_{p-1}(t) \oplus \sigma_0(t)$. Hence, if $p-1 > h > 0$ then the only possible quotients of $I_h(t)$ are $I_h(t), \sigma_{p-1-h}(t+h)$, and the trivial

quotient, and if $h = p-1$ then $I_h(t) = I_{p-1}(t) = \sigma_{p-1}(t) \oplus \sigma_0(t)$ so there is the additional possible quotient $\sigma_0(t)$. ☐

Lemma 20. *Let $r \geqslant (m+1)(p+1)$, and suppose that $a \in \overline{\mathbb{Q}}_p$ is such that $m+1 > v(a) > m$. Then $\overline{\Theta}_{r+2,a}$ is a quotient of $\sigma_r/\langle \overline{\theta}^{m+1}\sigma_{r-(m+1)(p+1)}, y^r, xy^{r-1}, \ldots, x^m y^{r-m}\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}$. This module has a series whose factors are $I_r, I_{r-2}(1), \ldots, I_{r-2m}(m)$, and consequently $\overline{\Theta}_{r+2,a}$ has a series whose factors are $M_0, \ldots, M_m$, where M_α is a quotient of a submodule of $I_{r-2\alpha}(\alpha)$, for each $0 \leqslant \alpha \leqslant m$.*

Proof. Follows from the facts that $\sigma_r/\overline{\theta}^{m+1}\sigma_{r-(m+1)(p+1)}$ has a series whose factors are

$$N_\alpha = \overline{\theta}^{\alpha}\sigma_{r-\alpha(p+1)}/\overline{\theta}^{\alpha+1}\sigma_{r-(\alpha+1)(p+1)} \cong I_{r-2\alpha}(\alpha),$$

for $0 \leqslant \alpha \leqslant m$, and each N_α has a submodule $N'_\alpha \subseteq N_\alpha$ such that

$$\begin{aligned} N'_\alpha &\cong \sigma_{\widetilde{r-2\alpha}}(\alpha), \\ N_\alpha/N'_\alpha &\cong \sigma_{(2\alpha - r \bmod p-1)}(r-\alpha), \end{aligned}$$

due to parts (a) and (c) of lemma 3.2 in [1]. ☐

2.3 Identities involving binomial sums

Lemma 21. *Let $t \geqslant 0$ be an integer, and suppose that $r = t(p-1)+s$, with $s \in \{1, \ldots, p-1\}$. Then:*

1. $\sum_{j=1}^t \binom{r}{j(p-1)} \equiv \frac{t}{s}p \pmod{p^2}$;
2. $$\textstyle\sum_{j=1}^t \binom{r}{j(p-1)} \equiv \frac{t}{s}p + p^2\left(tA_s + t^2 B_s\right) \pmod{p^3},$$
   where A_s and B_s depend only on s;
3. *If $s \neq 1$, then* $\sum_{j=1}^t j\binom{r}{j(p-1)} \equiv 0 \pmod{p}$;
4. *If $s \neq 1$ and if $p \mid t$, then* $\sum_{j=1}^t p^{-1} j\binom{r}{j(p-1)} \equiv 0 \pmod{p}$;
5. *If $A \geqslant 0$, then* $\sum_j \binom{r}{j(p-1)+A} \equiv \binom{s}{A \bmod p-1}(1 + \delta_{s=p-1}\delta_{A \equiv_{p-1} 0}) \pmod{p}$;
6. *If $A \in \mathbb{Z}$, and $R \geqslant 0$, and $M_{R,A} = \sum_j \binom{R}{j(p-1)+A}$, then*

$$M_{R,A} = \begin{cases} \sum_{i=0}^{R-1}\binom{R-1-i}{A-1}M_{i,0} & \text{if } A > 0, \\ \sum_{i=0}^{-A}(-1)^i\binom{-A}{i}M_{R-i,0} & \text{if } A < 0. \end{cases}$$

Proof. 1. For all $r \geqslant 1$, define M_r by the equation $M_r = \sum_{j=1}^t \binom{r}{j(p-1)}$. We want to show that $M_r = \frac{t}{s}p + O(p^2)$, where the valuation of the expression $O(p^2)$ is at least 2. We are going to prove this by induction. Note that $M_r = 0$ for $1 \leqslant i \leqslant p-1$, and $M_p = \binom{p}{p-1} = \frac{1}{1}p$, so the claim holds true when $1 \leqslant r \leqslant p$. Consequently, the base case of the induction holds true. Moreover, note that

$$M_r = (p-1)^{-1}\textstyle\sum_{\mu \in \mathbb{F}_p^\times}(1+[\mu])^r - 1 - \delta_{s=p-1},$$

for all $r \geqslant 1$. Let f be the polynomial of degree $p-2$ whose roots are the numbers $1+[\mu]$, so that $f(x) = \frac{1}{x}((x-1)^{p-1}-1) = a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_0$, and the coefficients of f are given by $a_{p-1-m} = (-1)^{m-1}\binom{p-1}{m-1}$. Then $N_r = M_r + 1 + \delta_{s=p-1}$ must satisfy the recurrence $N_{r+p-2} = -a_{p-3}N_{r+p-3} - \cdots - a_0 N_r$, for all $r \geqslant 1$. As $a_{p-3} + \cdots + a_0 = f(1) - 1 = -2$, then

$$M_{r+p-2} - 1 + (-1)^{s-1}\binom{p-1}{s-1} = \binom{p-1}{1}M_{r+p-3} - \cdots + \binom{p-1}{p-2}M_r,$$

for all $r \geqslant 1$. Note that $(-1)^{s-1}\binom{p-1}{s-1} = \frac{(s-1)!}{(s-1)!} - \frac{(s-1)!}{(s-1)!}\left(1^{-1} + \cdots + (s-1)^{-1}\right)p + O(p^2)$. Define $M'_r = \frac{t}{s}$. Then

$$\begin{aligned} M_{r+p-2} &= \left(-M'_{r+p-3} - \cdots - M'_r + \tfrac{1}{1} + \cdots + \tfrac{1}{s-1}\right)p + O(p^2) \\ &= \left(-M'_{r+p-3} - \cdots - M'_r - \tfrac{1}{s} - \cdots - \tfrac{1}{p-1}\right)p + O(p^2). \end{aligned}$$

If $s = 1$, then, by the induction hypothesis,

$$\begin{aligned} M_{r+p-2} &= \left(-M'_{r+p-3} - \cdots - M'_r - \tfrac{1}{s} - \cdots - \tfrac{1}{p-1}\right)p + O(p^2) \\ &= \left(-\tfrac{t}{p-2} \cdots - \tfrac{t}{1} - \tfrac{1}{1} - \cdots - \tfrac{1}{p-1}\right)p + O(p^2) = \tfrac{t}{p-1}p + O(p^2). \end{aligned}$$

If $s > 1$, then, by the induction hypothesis,

$$\begin{aligned} M_{r+p-2} &= \left(-M'_{r+p-3} - \cdots - M'_r - \tfrac{1}{s} - \cdots - \tfrac{1}{p-1}\right)p + O(p^2) \\ &= \left(-\tfrac{t+1}{s-2} - \cdots - \tfrac{t+1}{1} - \tfrac{t}{p-1} \cdots - \tfrac{t}{s+1} - \tfrac{t}{s} - \tfrac{1}{s} - \cdots - \tfrac{1}{p-1}\right)p + O(p^2) \\ &= \left(-\tfrac{t+1}{s-2} - \cdots - \tfrac{t+1}{1} - \tfrac{t+1}{p-1} \cdots - \tfrac{t+1}{s+1} - \tfrac{t+1}{s}\right)p + O(p^2) = \tfrac{t+1}{s-1}p + O(p^2). \end{aligned}$$

This completes the proof by induction that $M_r = \frac{t}{s}p + O(p^2)$, for all $r \geqslant 1$, which is equivalent to the first claim stated in the lemma.

2. Suppose that α_r is such that $M_r \equiv \frac{t}{s}p + p^2\alpha_r \pmod{p^3}$. These constants are unique up to addition of an $O(p)$ term, in the sense that α'_r is such that $M_r \equiv \frac{t}{s}p + p^2\alpha'_r \pmod{p^3}$ if and only if $\alpha'_r = \alpha_r + O(p)$. We know that there is the recurrence relation

$$M_{r+p-2} - 1 + (-1)^{s-1}\tbinom{p-1}{s-1} = \tbinom{p-1}{1}M_{r+p-3} - \cdots + \tbinom{p-1}{p-2}M_r,$$

for all $r \geqslant 1$. Consequently,

$$\begin{aligned} &\tfrac{t+1}{s-1}p + p^2(\alpha_{r+p-2} + \cdots + \alpha_r) \\ &\quad = p\left(\tfrac{1}{1} + \cdots + \tfrac{1}{s-1}\right) - p^2 \textstyle\sum_{1 \leqslant i < j \leqslant s-1} \tfrac{1}{ij} \\ &\qquad - \textstyle\sum_{i=1}^{s-2} \tfrac{t+1}{s-1-i}\left(p - p^2 \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k}\right) - \textstyle\sum_{i=s-1}^{p-2} \tfrac{t}{p+s-2-i}\left(p - p^2 \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k}\right) + O(p^3) \\ &\quad = \tfrac{t+1}{s-1}p - pt\textstyle\sum_{k=1}^{p-1} \tfrac{1}{k} - p^2 \textstyle\sum_{1 \leqslant i < j \leqslant s-1} \tfrac{1}{ij} + p^2 \textstyle\sum_{i=1}^{s-2} \tfrac{t+1}{s-1-i} \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k} \\ &\qquad + p^2 \textstyle\sum_{i=s-1}^{p-2} \tfrac{t}{p+s-2-i} \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k} + O(p^3) \\ &\quad = \tfrac{t+1}{s-1}p + p^2(A'_s + tB'_s) + O(p^3), \end{aligned}$$

where

$$\begin{aligned} A'_s &= -\textstyle\sum_{1 \leqslant i < j \leqslant s-1} \tfrac{1}{ij} + \textstyle\sum_{i=1}^{s-2} \tfrac{1}{s-1-i} \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k}, \\ B'_s &= -\tfrac{1}{p}\textstyle\sum_{k=1}^{p-1} \tfrac{1}{k} + \textstyle\sum_{i=1}^{s-2} \tfrac{1}{s-1-i} \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k} + \textstyle\sum_{i=s-1}^{p-2} \tfrac{1}{p+s-2-i} \textstyle\sum_{1 \leqslant k \leqslant i} \tfrac{1}{k}. \end{aligned}$$

Therefore, $\alpha_{r+p-1} - \alpha_r = A''_s + tB''_s + O(p)$. Hence there is the recurrence relation

$$\alpha_{r+3(p-1)} - 3\alpha_{r+2(p-1)} + 3\alpha_{r+(p-1)} - \alpha_r = O(p).$$

This implies that there are constants A_s, B_s, γ_s, such that

$$\alpha_r = \alpha_{t(p-1)+s} = \gamma_s + tA_s + t^2B_s + O(p).$$

Since $M_1 = \cdots = M_{p-1} = 0$ and $M_p = p$, we have $\alpha_1 = \cdots = \alpha_p = O(p)$, which implies that

$\gamma_s = 0$. This completes the proof of the second part of the lemma.

3. For all $r \geqslant 1$, define L_r by $L_r = \sum_{j=1}^{t} j\binom{r}{j(p-1)}$. We want to show that $p \mid L_r$, when $s \neq 1$. Note that

$$\begin{aligned} -r\sum_{u\in\mathbb{F}_p^\times} u(1+u)^{r-1} &= -r\sum_{m=0}^{r-1}\binom{r-1}{m}\sum_{u\in\mathbb{F}_p^\times} u^{m+1} \\ &= -\sum_{m=1}^{r} m\binom{r}{m}\sum_{u\in\mathbb{F}_p^\times} u^m = L_r + r\delta_{s=p-1}, \end{aligned}$$

in $\mathbb{F}_p$. Consequently,

$$\begin{aligned} L_r &= -r\sum_{u\in\mathbb{F}_p^\times} u(1+u)^{r-1} - r\delta_{s=p-1} \\ &= -r\left(\sum_{u\in\mathbb{F}_p^\times} u(1+u)^{s-1} + \delta_{s=p-1}\right) = \tfrac{r}{s}L_s, \end{aligned}$$

in $\mathbb{F}_p$. As $L_s =$ empty sum $= 0$, then $L_r = 0$ in $\mathbb{F}_p$ as well, when $s \neq 1$.

4. By the first part of this proof, the claim we want to show is equivalent to the congruence $\sum_{j=1}^{t} j(p-1)\binom{r}{j(p-1)} \equiv 0 \pmod{p^2}$. Note that

$$\begin{aligned} \sum_{j=1}^{t} j(p-1)\binom{r}{j(p-1)} &\equiv r\sum_{j=1}^{t}\binom{r-1}{j(p-1)-1} \\ &\equiv r\sum_{j=1}^{t}\binom{r}{j(p-1)} - r\sum_{j=1}^{t}\binom{r-1}{j(p-1)} \equiv 0 \pmod{p^2}, \end{aligned}$$

the last part being true due to the second part of this lemma and the fact that $s > 1$.

5. Let $r = t(p-1)+s$, with $t \geqslant 0$ and $s \in \{1,\ldots,p-1\}$, and let $\nu = A \bmod p-1$. Then, in $\mathbb{F}_p$,

$$\sum_j \binom{r}{j(p-1)+A} = -\sum_{u\in\mathbb{F}_p^\times} u^{-\nu}(1+u)^r = -\sum_{u\in\mathbb{F}_p^\times} u^{-\nu}(1+u)^s = \binom{s}{\nu}(1+\delta_{s=p-1,\nu=0}).$$

6. Follows from a repeated application of the identity $M_{R,B} = M_{R-1,B} + M_{R-1,B-1}$, which holds true whenever $R, B \geqslant 0$.

□

Lemma 22. *Let $r, L, b, N \geqslant 0$ be integers, and suppose that $r \geqslant (L+b)N$. Then:*

1. $\sum_j (-1)^{j-b}\binom{L}{j-b}\binom{r-jN}{u} = \delta_{u=L}N^L$, for all $0 \leqslant u \leqslant L$.

Proof. Let $t = \lfloor r/N \rfloor - b$. For all $u, L \geqslant 0$, define $M_{u,L}$ by the equation

$$M_{u,L} = \sum_j (-1)^{j-b}\binom{L}{j-b}\binom{r-jN}{u},$$

and let $f(x,y)$ denote the polynomial $f(x,y) = \sum_{r\geqslant u\geqslant 0, t\geqslant L\geqslant 0} M_{u,L}x^L y^u$. Then

$$\begin{aligned} f(x,y) &= \sum_{r\geqslant u\geqslant 0, t\geqslant L\geqslant 0} M_{u,L}x^L y^u = \sum_{j\geqslant 0, r\geqslant u\geqslant 0, t\geqslant L\geqslant 0} x^L\binom{L}{j-b}(-1)^{j-b}\binom{r-jN}{u}y^u \\ &= \sum_{j\geqslant 0, t\geqslant L\geqslant 0} x^L\binom{L}{j-b}(-1)^{j-b}(1+y)^{r-jN} \\ &= (1+y)^{r-(L+b)N}\sum_{j\geqslant 0, t\geqslant L\geqslant 0} x^L\binom{L}{j-b}(-1)^{j-b}(1+y)^{(L-(j-b))N} \\ &= (1+y)^{r-(L+b)N}\sum_{t\geqslant L\geqslant 0} x^L((1+y)^N-1)^L \\ &= (1-x((1+y)^N-1))^{-1}(1+y)^{r-(L+b)N}(1-(x((1+y)^N-1))^{t+1}) \\ &= (1-Nxy-xy^2h_3(y))^{-1}(1+h_1(y))(1-N^{t+1}x^{t+1}y^{t+1}-x^{t+1}y^{t+2}h_4(y)), \end{aligned}$$

where the h_i are polynomials, so

$$\begin{aligned}\lim_{\epsilon\to 0} f(\epsilon^{-1}x,\epsilon) &= \lim_{\epsilon\to 0}(1-Nx+O(\epsilon))^{-1}(1+O(\epsilon))(1-N^{t+1}x^{t+1}+O(\epsilon))\\ &= \lim_{\epsilon\to 0}(1-Nx+O(\epsilon))^{-1}(1-N^{t+1}x^{t+1}+O(\epsilon))\\ &= (1-Nx)^{-1}(1-N^{t+1}x^{t+1}) = \textstyle\sum_{j=0}^{t} N^j x^j.\end{aligned}$$

Since this is still a polynomial in x, it follows that $M_{u,L}=0$ whenever $0\leqslant u<L$. Moreover,

$$[x^L y^L]f(x,y) = [x^L]\lim_{\epsilon\to 0} f(\epsilon^{-1}x,\epsilon) = N^L,$$

whenever $0\leqslant L\leqslant t$. □

Lemma 23. *1. Let $A,z,w\geqslant 0$ be integers. Then* $\binom{z}{w}=\sum_v(-1)^{w-v}\binom{A+w-v-1}{w-v}\binom{z+A}{v}$.

2. Let $A,i,w\geqslant 0$ be integers. Then $\binom{i}{w}\equiv\sum_v(-1)^v\binom{A-v}{w-v}\binom{i(p-1)+A}{v} \pmod{p}$.

Proof. 1. Let $L_z=\sum_w X^w\sum_v(-1)^{w-v}\binom{A+w-v-1}{w-v}\binom{z+A}{v}$. Then

$$\begin{aligned}L_z &= \textstyle\sum_v(-1)^v\binom{z+A}{v}\sum_{w\geqslant v}X^w(-1)^w\binom{A+w-v-1}{w-v} = \sum_v X^v\binom{z+A}{v}\sum_u(-X)^u\binom{A+u-1}{u}\\ &= (1+X)^{z+A}(1-(-X))^{-A} = (1+X)^z = \textstyle\sum_w X^w\binom{z}{w}.\end{aligned}$$

Consequently, $\binom{z}{w}=[X^w]\sum_w X^w\binom{z}{w}=[X^w]L_z=\sum_v(-1)^{w-v}\binom{A+w-v-1}{w-v}\binom{z+A}{v}$.

2. Let $L'_z=\sum_w X^w\sum_v(-1)^v\binom{A-v}{w-v}\binom{A-i}{v}$. Then

$$\begin{aligned}L'_z &= \textstyle\sum_v(-1)^v\binom{A-i}{v}\sum_{w\geqslant v}X^w\binom{A-v}{w-v} = \sum_v(-X)^v\binom{A-i}{v}\sum_u X^u\binom{A-v}{u}\\ &= (1+X)^i\textstyle\sum_v\binom{A-i}{v}(-X)^v(1+X)^{A-i-v} = (1+X)^i = \sum_w X^w\binom{i}{w}.\end{aligned}$$

Consequently, $\binom{i}{w}=[X^w]\sum_w X^w\binom{i}{w}=[X^w]L'_z=\sum_v(-1)^v\binom{A-v}{w-v}\binom{A-i}{v}$.

□

Lemma 24. *Let $r,\alpha,\beta,\gamma\geqslant 0$ be integers, and suppose that $m\geqslant\alpha(p+1)+\beta(p-1)+\gamma$, and $\beta\geqslant\alpha>0$, and $C_j\in\mathbb{Z}$. Then*

$$f=\textstyle\sum_{j=0}^{\beta}C_jx^{\alpha+\gamma+j(p-1)}y^{r-\alpha-\gamma-j(p-1)} = (-1)^\alpha\sum_{j=0}^{\beta-\alpha}C_j^{(\alpha)}\theta^\alpha x^{\gamma+j(p-1)}y^{r-\alpha(p+1)-\gamma-j(p-1)},$$

for some $C_j^{(\alpha)}\in\mathbb{Z}$, if and only if $\sum_{j=0}^{\beta}C_j\binom{j}{w}=0$ for all $0\leqslant w<\alpha$. Moreover, in that case $C'_{\beta-\alpha}=C_\beta$, and $C'_0=(-1)^\alpha C_0$, and

$$C_j^{(\alpha)}=(-1)^\alpha\textstyle\sum_{i=j+1}^{\beta}\binom{i-j-1}{\alpha-1}C_i,$$

and consequently

$$\textstyle\sum_{j=0}^{\beta-\alpha}C_j^{(\alpha)}=(-1)^\alpha\sum_{j=0}^{\beta}C_j\binom{j}{\alpha}.$$

Proof. We will prove this by induction on $\alpha>0$. In the base case $\alpha=1$, the induction hypothesis is equivalent to the fact that

$$f=\textstyle\sum_{j=0}^{\beta}C_jx^{1+\gamma+j(p-1)}y^{r-1-\gamma-j(p-1)} = -\sum_{j=0}^{\beta-1}C_j^{(1)}\theta x^{\gamma+j(p-1)}y^{r-(p+1)-\gamma-j(p-1)},$$

for some $C_j^{(1)}\in\mathbb{Z}$, if and only if $\sum_{j=0}^{\beta}C_j=0$, and $C_j^{(1)}=-\sum_{i=j+1}^{\beta}C_i$. Indeed, if the right side is expanded into the left side, then $\sum_{j=0}^{\beta}C_j=0$ and $C_j^{(1)}=-\sum_{i=j+1}^{\beta}C_i$, and conversely if $\sum_{j=0}^{\beta}C_j=0$ then the left side can be grouped into the right side, and $C_j^{(1)}=-\sum_{i=j+1}^{\beta}C_i$ due to uniqueness of the coefficients. Suppose that the induction hypothesis holds true for all

$\alpha' < \alpha$. Then

$$f = \sum_{j=0}^{\beta} C_j x^{\alpha+\gamma+j(p-1)} y^{r-\alpha-\gamma-j(p-1)} = (-1)^\alpha \sum_{j=0}^{\beta-\alpha} C_j^{(\alpha)} \theta^\alpha x^{\gamma+j(p-1)} y^{r-\alpha(p+1)-\gamma-j(p-1)},$$

for some $C_j^{(\alpha)} \in \mathbb{Z}$, if and only if the following four conditions hold true:

$$\begin{aligned} \textstyle\sum_{j=0}^{\beta} C_j \binom{j}{w} &= 0 \text{ for all } 0 \leqslant w < \alpha - 1, \\ C_j^{(\alpha-1)} &= -(-1)^\alpha \textstyle\sum_{i=j+1}^{\beta} \binom{i-j-1}{\alpha-2} C_i, \\ \textstyle\sum_{j=0}^{\beta} C_j^{(\alpha-1)} &= 0, \\ C_j^{(\alpha)} &= -\textstyle\sum_{i=j+1}^{\beta} C_i^{(\alpha-1)}. \end{aligned}$$

These conditions can be combined into the folowing two conditions:

$$\begin{aligned} \textstyle\sum_{j=0}^{\beta} C_j \binom{j}{w} &= 0 \text{ for all } 0 \leqslant w < \alpha, \\ C_j^{(\alpha)} &= (-1)^\alpha \textstyle\sum_{s=j+2}^{\beta} C_s \sum_{i \geqslant j+1} \binom{s-i-1}{\alpha-2} \\ &= (-1)^\alpha \textstyle\sum_{s=j+2}^{\beta} \binom{s-j-1}{\alpha-1} C_s = (-1)^\alpha \sum_{s=j+1}^{\beta} \binom{s-j-1}{\alpha-1} C_s. \end{aligned}$$

This completes the proof by induction. The facts that $C'_{\beta-\alpha} = C_\beta$ and $C'_0 = (-1)^\alpha C_0$ can be deduced by comparing the top and bottom coefficients in the two expressions of f. ☐

Lemma 25. *Let $r, m, L, l, w \geqslant 0$ be integers. Suppose that $r \geqslant (m+1)(p+1)$, and $r \equiv_{p-1} 2L$, and $1 \leqslant L \leqslant m$, and $p > m+1$. Then*

$$\textstyle\sum_i \binom{r-m+l}{i(p-1)+l} \binom{(p-1)i}{w} \equiv \sum_{v=0}^{w} \kappa_v \binom{r-m+l}{v} \pmod{p},$$

where $\kappa_v = (-1)^{w-v} \binom{l+w-v-1}{w-v} \eta(2L - m + l - v, l - v)$, where

$$\eta(X, Y) = \begin{cases} \binom{X}{Y} & \text{if } X \geqslant 1, \\ (1 + \delta_{X=Y=0}) \binom{X-1}{Y} & \text{if } X < 1 \text{ and } Y \geqslant 0, \\ \binom{X-1}{X-Y} & \text{if } X < 1 \text{ and } Y < 0. \end{cases}$$

Similarly,

$$\textstyle\sum_i \binom{r-m+l}{i(p-1)+l} \binom{i}{w} \equiv \sum_{v=0}^{w} \kappa'_v \binom{r-m+l}{v} \pmod{p},$$

where $\kappa'_v = (-1)^v \binom{l-v}{w-v} \eta(2L - m + l - v, l - v)$.

Proof. Note that $\binom{i(p-1)}{w} = \sum_v (-1)^{w-v} \binom{l+w-v-1}{w-v} \binom{i(p-1)+l}{v}$, due to lemma 21. Consequently,

$$\begin{aligned} \textstyle\sum_i \binom{r-m+l}{i(p-1)+l} \binom{i(p-1)}{w} &= \textstyle\sum_i \binom{r-m+l}{i(p-1)+l} \sum_v (-1)^{w-v} \binom{l+w-v-1}{w-v} \binom{i(p-1)+l}{v} \\ &= \textstyle\sum_v (-1)^{w-v} \binom{l+w-v-1}{w-v} \binom{r-m+l}{v} \sum_i \binom{r-m+l-v}{i(p-1)+l-v} \\ &\equiv \textstyle\sum_v (-1)^{w-v} \binom{l+w-v-1}{w-v} \binom{r-m+l}{v} (1 + \delta_{2L+l=m+v} \delta_{l=v}) \binom{2L\widetilde{-m+l}-v}{l-v \bmod p-1} \\ &\equiv \textstyle\sum_v (-1)^{w-v} \binom{l+w-v-1}{w-v} \binom{r-m+l}{v} \eta(2L - m + l - v, l - v) \pmod{p}. \end{aligned}$$

The proof of the second part is similar, and uses the second part of lemma 21. ☐

3 General theorems

3.1 The main theorems

The main results in this section are the following two theorems.

Theorem 26. *Let $r, m, \alpha \geqslant 0$ be such that $r \geqslant (m+1)(p+1)$, and $m \geqslant \alpha$, and $r \equiv_{p-1} 2L$, with $L \in \{1, \ldots, m\}$. Let $a \in \overline{\mathbb{Q}}_p$ be such that $m+1 > v(a) > m$. Define the $(\alpha+1) \times (m+1+\mu)$ matrix $\mathfrak{M}^{(r,m,\alpha)}$, where $\omega_1 < \cdots < \omega_\mu$ are such that*

$$\{\omega_1, \ldots, \omega_\mu\} = \{j \mid j(p-1) + \alpha \in [\alpha, m] \cup [r-m, r-\alpha]\},$$

by

$$\mathfrak{M}^{(r,m,\alpha)}_{u,j} = \tbinom{\omega_j}{u-1} - \delta_{u=\alpha+1}((-1)^\alpha \delta_{j=1} + \delta_{j=\mu}\delta_{L\equiv_{p-1}\alpha}),$$

whenever $1 \leqslant j \leqslant \mu$, and

$$\mathfrak{M}^{(r,m,\alpha)}_{u,l+m-\alpha+1+\mu} = \textstyle\sum_{r-m>i(p-1)+\alpha>m} \tbinom{r-\alpha+l}{i(p-1)+l}\tbinom{i}{u-1}.$$

Suppose that $(0, \ldots, 0, 1)^T$ is in the range of $\mathfrak{M}^{(r,m,\alpha)}$ over $\mathbb{F}_p$. Then (the map induced by) Ψ_α, restricted to $X(r+2,a)$, is a surjective map

$$\Psi_\alpha|_{X(r+2,a)} : I(\overline{\theta}^\alpha \sigma_{r-\alpha(p+1)}) \cap X(r+2,a) \subseteq I(\sigma_r) \twoheadrightarrow I(\sigma_{(2\alpha-r \bmod p-1)}(r-\alpha)).$$

Theorem 27. *Let $r, m, \alpha \geqslant 0$ be integers such that $r > m(p+1)$, and $m > \alpha$, and $r \equiv_{p-1} 2L$, with $L \in \left\{1, \ldots, \frac{p-1}{2}\right\}$. Let $a \in \overline{\mathbb{Q}}_p$ be such that $m+1 > v(a) > m$. For $w \geqslant 0$, define*

$$\mathfrak{m}_w(C_1, \ldots, C_\alpha) = \textstyle\sum_{r-2\alpha>i(p-1)>0} \sum_{l=0}^{\alpha} C_l \tbinom{r-\alpha+l}{i(p-1)+l}\tbinom{i}{w},$$

where $C_0 = 1$. Denote by $\mathfrak{v}_w(C_1, \ldots, C_\alpha)$ the valuation $v(\mathfrak{m}_w(C_1, \ldots, C_\alpha))$. Suppose that the following three conditions hold true:

1. *$\mathfrak{m}_w(C_1, \ldots, C_\alpha) = 0$, for all $0 \leqslant w < \alpha$;*
2. *$\min\{v(a) - \alpha, \mathfrak{v}_\alpha(C_1, \ldots, C_\alpha)\} \leqslant \mathfrak{v}_w(C_1, \ldots, C_\alpha)$, for all $\alpha < w \leqslant 2m+1-\alpha$;*
3. *If $L \equiv_{p-1} \alpha$ and $v(a) - \alpha < \mathfrak{v}_\alpha(C_1, \ldots, C_\alpha)$, then $\sum_{l=0}^{\alpha} C_l \binom{r-\alpha+l}{\alpha} \equiv (-1)^{\alpha+1} \pmod{p}$.*

— *If $\mathfrak{v}_\alpha(C_1, \ldots, C_\alpha) < v(a) - \alpha$, then*

$$\Psi_\alpha|_{X(r+2,a)} : I(\overline{\theta}^\alpha \sigma_{r-\alpha(p+1)}) \cap X(r+2,a) \subseteq I(\sigma_r) \twoheadrightarrow I(\sigma_{(2\alpha-r \bmod p-1)}(r-\alpha))$$

is a surjection;

— *If $\mathfrak{v}_\alpha(C_1, \ldots, C_\alpha) > v(a) - \alpha$, then*

$$\Psi_\alpha\left(I(\overline{\theta}^\alpha \sigma_{r-\alpha(p+1)}) \cap X(r+2,a)\right) \supseteq T\left(I(\sigma_{(2\alpha-r \bmod p-1)}(r-\alpha))\right).$$

3.2 Proof of theorem 26

3.2.1 Lemmas

Lemma 28. *Let $r, m, n, \alpha, \beta \geqslant 0$ be integers, and let $a \in \overline{\mathbb{Q}}_p$ be such that $m+1 > v(a) > m$. Suppose that $n \geqslant m+1$, and $n \geqslant \alpha$, and $p-1 > \beta$, and $r \geqslant np + \alpha$. Then there is some*

$\tau^{\star}_{r,m,n,\alpha,\beta}$ *such that*

$$
\begin{aligned}
&(T-a)\tau^{\star}_{r,m,n,\alpha,\beta}\\
&\quad\equiv \textstyle\sum_i \left[1, x^{i(p-1)+\alpha-\beta}y^{r-i(p-1)-\alpha+\beta}\right] \sum_{j<i}(-1)^j\binom{n}{j}\binom{r-j(p-1)-\alpha}{(i-j)(p-1)-\beta}p^{j(p-1)+\alpha}(p-1)\\
&\qquad + (p-1)(-1)^{\alpha+1}\delta_{r\equiv_{p-1}2\alpha}\textstyle\sum_j(-1)^j\binom{n}{j}p^{j(p-1)+\alpha}\left[1, y^{j(p-1)+\alpha}x^{r-j(p-1)-\alpha}\right]\\
&\qquad - a\textstyle\sum_j(-1)^j\binom{n-\alpha}{j}\sum_\mu[\mu]^\beta\left[\left(\begin{smallmatrix} p & [\mu]\\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right]\\
&\qquad - a\textstyle\sum_j(-1)^j\binom{n-\alpha}{j}\delta_{r\equiv_{p-1}2\alpha}\left[\left(\begin{smallmatrix} 1 & 0\\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right] \pmod{p^{m+1}}.
\end{aligned}
$$

Proof. Take

$$\tau^{\star}_{r,m,n,\alpha,\beta} = \textstyle\sum_\mu[\mu]^\beta\phi^{*}_{r,m,n,\alpha,\left(\begin{smallmatrix} p & [\mu]\\ 0 & 1\end{smallmatrix}\right)} - p\delta_{\beta=0}\phi^{*}_{r,m,n,\alpha,\left(\begin{smallmatrix} p & 0\\ 0 & 1\end{smallmatrix}\right)} - (p-1)(-1)^\alpha\delta_{r\equiv_{p-1}2\alpha}\phi^{**}_{r,m,n,\alpha,\left(\begin{smallmatrix} 1 & 0\\ 0 & p\end{smallmatrix}\right)}.$$

Then

$$
\begin{aligned}
&(T-a)\tau^{\star}_{r,m,n,\alpha,\beta}\\
&\quad\equiv \textstyle\sum_j(-1)^j\binom{n}{j}p^{j(p-1)+\alpha}\sum_\mu[\mu]^\beta\left[\left(\begin{smallmatrix} 1 & [\mu]\\ 0 & 1\end{smallmatrix}\right), x^{j(p-1)+\alpha}y^{r-j(p-1)-\alpha}\right] - p\delta_{\beta=0}\phi^{*}_{r,m,n,\alpha,\left(\begin{smallmatrix} p & 0\\ 0 & 1\end{smallmatrix}\right)}\\
&\qquad + (p-1)(-1)^{\alpha+1}\delta_{r\equiv_{p-1}2\alpha}\textstyle\sum_j(-1)^j\binom{n}{j}p^{j(p-1)+\alpha}\left[1, y^{j(p-1)+\alpha}x^{r-j(p-1)-\alpha}\right]\\
&\qquad - a\textstyle\sum_j(-1)^j\binom{n-\alpha}{j}\sum_\mu[\mu]^\beta\left[\left(\begin{smallmatrix} p & [\mu]\\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right]\\
&\qquad - a\textstyle\sum_j(-1)^j\binom{n-\alpha}{j}\delta_{r\equiv_{p-1}2\alpha}\left[\left(\begin{smallmatrix} 1 & 0\\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right] \pmod{p^{m+1}}.
\end{aligned}
$$

Note that

$$
\begin{aligned}
&\textstyle\sum_j(-1)^j\binom{n}{j}p^{j(p-1)+\alpha}\sum_\mu[\mu]^\beta\left[\left(\begin{smallmatrix} 1 & [\mu]\\ 0 & 1\end{smallmatrix}\right), x^{j(p-1)+\alpha}y^{r-j(p-1)-\alpha}\right]\\
&\quad= \textstyle\sum_j(-1)^j\binom{n}{j}p^{j(p-1)+\alpha}\sum_\mu[\mu]^\beta\left[1, x^{j(p-1)+\alpha}(y+[\mu]x)^{r-j(p-1)-\alpha}\right]\\
&\quad= \textstyle\sum_{i,j}(-1)^j\binom{n}{j}\binom{r-j(p-1)-\alpha}{i}p^{j(p-1)+\alpha}\sum_\mu[\mu]^{i+\beta}\left[1, x^{j(p-1)+\alpha+i}y^{r-j(p-1)-\alpha-i}\right]\\
&\quad= \textstyle\sum_{i,j}(-1)^j\binom{n}{j}\binom{r-j(p-1)-\alpha}{i(p-1)-\beta}p^{j(p-1)+\alpha}(p-1+\delta_{i(p-1)=\beta})\\
&\qquad\times\left[1, x^{(i+j)(p-1)+\alpha-\beta}y^{r-(i+j)(p-1)-\alpha+\beta}\right]\\
&\quad= \textstyle\sum_{i,j}(-1)^j\binom{n}{j}\binom{r-j(p-1)-\alpha}{i(p-1)-\beta}p^{j(p-1)+\alpha}(p-1+\delta_{i=\beta=0})\\
&\qquad\times\left[1, x^{(i+j)(p-1)+\alpha-\beta}y^{r-(i+j)(p-1)-\alpha+\beta}\right]\\
&\quad= \textstyle\sum_{i,j}(-1)^j\binom{n}{j}\binom{r-j(p-1)-\alpha}{(i-j)(p-1)-\beta}p^{j(p-1)+\alpha}(p-1+\delta_{i=j})\\
&\qquad\times\left[1, x^{i(p-1)+\alpha-\beta}y^{r-i(p-1)-\alpha+\beta}\right]\\
&\quad\equiv \textstyle\sum_i\left[1, x^{i(p-1)+\alpha-\beta}y^{r-i(p-1)-\alpha+\beta}\right]\sum_{j<i}(-1)^j\binom{n}{j}\binom{r-j(p-1)-\alpha}{(i-j)(p-1)-\beta}p^{j(p-1)+\alpha}(p-1)\\
&\qquad + p\delta_{\beta=0}\phi^{*}_{r,m,n,\alpha,\left(\begin{smallmatrix} p & 0\\ 0 & 1\end{smallmatrix}\right)} \pmod{p^{m+1}}.
\end{aligned}
$$

The proof of the lemma can be completed by combining these two congruences. ☐

Lemma 29. *Let $r, m, n, \alpha \geqslant 0$ be integers, and let $a \in \overline{\mathbb{Q}}_p$ be such that $m+1 > v(a) > m$. Suppose that $n \geqslant m+1$, and $n \geqslant \alpha$, and $r \geqslant np+\alpha$. Then, for any $C_1, \ldots, C_\alpha \in \mathbb{Z}_p$, there is some $\tau^{\star\star}_{r,m,n,\alpha,C_1,\ldots,C_\alpha}$ such that*

$$
\begin{aligned}
&(T-a)\tau^{\star\star}_{r,m,n,\alpha,C_1,\ldots,C_\alpha}\\
&\quad\equiv \textstyle\sum_i D_i\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right]\\
&\qquad - a\textstyle\sum_j(-1)^j\binom{n-\alpha}{j}\sum_\mu\left[\left(\begin{smallmatrix} p & [\mu]\\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right]\\
&\qquad - a\textstyle\sum_j(-1)^j\binom{n-\alpha}{j}\delta_{r\equiv_{p-1}2\alpha}\left[\left(\begin{smallmatrix} 1 & 0\\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right] \pmod{p^{m+1}},
\end{aligned}
$$

where

$$(p-1)^{-1}D_i = \sum_{j<i}(-1)^j\binom{n}{j}p^{j(p-1)+\alpha}\left(\binom{r-j(p-1)-\alpha}{(i-j)(p-1)} + \sum_{l=1}^{\alpha} C_l\binom{r-j(p-1)-\alpha+l}{(i-j)(p-1)+l}\right)$$
$$+ (-1)^{\alpha+1}\delta_{r\equiv_{p-1}2\alpha}(-1)^{(r-2\alpha)/(p-1)-i}\binom{n}{(r-2\alpha)/(p-1)-i}p^{r-i(p-1)-\alpha}.$$

Proof. Write

$$\tau' = \sum_{\mu}[\mu]^{\beta}\phi^{*}_{r,m,n,\alpha,\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right)} - p\delta_{\beta=0}\phi^{*}_{r,m,n,\alpha,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)}$$

and

$$\tau'' = -(p-1)(-1)^{\alpha}\delta_{r\equiv_{p-1}2\alpha}\phi^{**}_{r,m,n,\alpha,\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)},$$

so that $\tau^{\star}_{r,m,n,\alpha,\beta} = \tau' + \tau''$. Take

$$\tau^{\star\star}_{r,m,n,\alpha,C_1,\dots,C_\alpha} = \tau^{\star}_{r,m,n,\alpha,0} + \sum_{l=1}^{\alpha} C_l p^l \tau'_{r,m,n,\alpha-l,(-l \bmod p-1)}.$$

It can be checked that $\tau^{\star\star}_{r,m,n,\alpha,C_1,\dots,C_\alpha}$ satisfies all of the requirements in the statement of the theorem. □

Corollary 30. *Let $r, m, \alpha \geqslant 0$ be integers, and let $a \in \overline{\mathbb{Q}}_p$ be such that $m+1 > v(a) > m$. Suppose that $m \geqslant \alpha$, and $r \geqslant (m+1)(p+1)$. Then, for any $F_j, C_0, \dots, C_m \in \mathbb{Z}_p$, there is some $\tau^{\dagger}_{r,m,\alpha,F_j,C_0,\dots,C_m}$ such that*

$$\begin{aligned}(T-a)&\tau^{\dagger}_{r,m,\alpha,F_j,C_0,\dots,C_m} \\ &\equiv \sum_{r-m>i(p-1)+\alpha>m} E_i\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right] \\ &\quad + \sum_{j(p-1)+\alpha\in[\alpha,m]\cup[r-m,r-\alpha]} F_j\left[1, x^{j(p-1)+\alpha}y^{r-j(p-1)-\alpha}\right] \pmod{p^{v(a)-m}},\end{aligned}$$

where $E_i = \sum_{l=\alpha-m}^{\alpha} C_{l+m-\alpha}\binom{r-\alpha+l}{i(p-1)+l}$.

Proof. Define τ' as in the proof of lemma 29. Take

$$\tau^{\dagger}_{r,m,\alpha,F_j,C_0,\dots,C_m} = (p-1)^{-1}p^{-m}\sum_{l=\alpha-m}^{\alpha} C_{l+m-\alpha}p^{l+m-\alpha}\tau'_{r,m,m+1,\alpha-l,(-l \bmod p-1)}$$
$$+ \sum_{u=0}^{m} X_u p^{-u}\phi^{*}_{r,m,m+1,u,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)} + \sum_{u=0}^{m} Y_u p^{-u}\phi^{**}_{r,m,m+1,u,\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)},$$

with suitably chosen constants $X_u, Y_u \in \mathbb{Z}_p$. □

3.2.2 Completing the proof of theorem 26

Proof of theorem 26. Let $n = m+1$. Since $(0,\dots,0,1)^T$ is in the range of $\mathfrak{M}^{(r,m,\alpha)}$ over $\mathbb{F}_p$, the constants $F_j, C_l \in \mathbb{Z}_p$ in lemma 30 can be chosen to be such that

$$\sum_{j=1}^{\mu} F_{\omega_j}\left(\binom{\omega_j}{u-1} - \delta_{u=\alpha+1}((-1)^{\alpha}\delta_{j=1} + \delta_{j=\mu}\delta_{L\equiv_{p-1}\alpha})\right)$$
$$+ \sum_{l=\alpha-m}^{\alpha}\sum_{r-m>i(p-1)+\alpha>m} C_l\binom{r-\alpha+l}{i(p-1)+l}\binom{i}{u-1} = \delta_{u=\alpha+1},$$

or, equivalently,

$$\sum_{j=1}^{\mu} F_{\omega_j}\binom{\omega_j}{u-1} + \sum_{l=\alpha-m}^{\alpha}\sum_{r-m>i(p-1)+\alpha>m} C_l\binom{r-\alpha+l}{i(p-1)+l}\binom{i}{u-1}$$
$$= \delta_{u=\alpha+1}(1 + (-1)^{\alpha}F_{\omega_1} + \delta_{L=2\alpha}F_{\omega_\mu}).$$

This implies that the constants $F_j, E_i \in \mathbb{Z}_p$ are such that

$$\begin{aligned}\textstyle\sum_{r-m>i(p-1)+\alpha>m} E_i \left[1, x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha}\right] \\ + \textstyle\sum_{j(p-1)+\alpha\in[\alpha,m]\cup[r-m,r-\alpha]} F_j \left[1, x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha}\right] \\ = \textstyle\sum_i E'_i \left[1, \theta^\alpha x^{i(p-1)} y^{r-\alpha(p+1)-i(p-1)}\right],\end{aligned}$$

for some constants $E'_i \in \mathbb{Z}_p$ which add up to

$$1 + (-1)^\alpha F_{\omega_1} + \delta_{L\equiv_{p-1}\alpha} F_{\omega_\mu}.$$

Moreover,

$$\begin{aligned}E'_0 &= (-1)^\alpha F_{\omega_1}, \\ E'_{(r-\alpha(p+1))/(p-1)} &= F_{\omega_\mu} \text{ whenever } L \equiv_{p-1} \alpha.\end{aligned}$$

This implies that $(T-a)\tau^\dagger_{r,m,n,\alpha,F_j,C_0,\ldots,C_m}$ is in the domain of (the map induced by) Ψ_α, and

$$\overline{(T-a)\tau^\dagger_{r,m,n,\alpha,F_j,C_0,\ldots,C_m}} = \textstyle\sum_i E'_i \left[1, \overline{\theta}^\alpha x^{i(p-1)} y^{r-\alpha(p+1)-i(p-1)}\right],$$

which implies that $\Psi_\alpha(\overline{(T-a)\tau^\dagger_{r,m,n,\alpha,F_j,C_0,\ldots,C_m}}) = \left[1, X^{(2\alpha-r \bmod p-1)}\right]$. The fact that the module $\sigma_{(2\alpha-r \bmod p-1)}(r-\alpha)$ is simple and hence generated by $X^{(2\alpha-r \bmod p-1)}$ completes the proof of the theorem. □

Remark. Theorem 26 can be proved similarly by using lemma 18 instead of corollary 30.

3.3 Proof of theorem 27

Proof of theorem 27. We know, from the proof of lemma 16, that

$$\begin{aligned}(T-a)\phi^{(0)}_{\alpha+1,\alpha,1} &\equiv \textstyle\sum_{z=\alpha+1}^m p^z \sum_j (-1)^j \binom{\alpha+1}{j}\binom{r-j(p-1)-\alpha}{z} \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z} \left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right] \\ &\quad + \textstyle\sum_j (-1)^j \binom{\alpha+1}{j} p^{r-j(p-1)-\alpha} \left[\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right), x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha}\right] \\ &\quad + \textstyle\sum_j (-1)^j \binom{\alpha+1}{j} p^{j(p-1)+\alpha} \left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha}\right] \\ &\quad - a \textstyle\sum_j (-1)^j \binom{1}{j} \left[1, \theta^\alpha x^{j(p-1)} y^{r-\alpha(p+1)-j(p-1)}\right] \\ &\equiv \textstyle\sum_{z=\alpha+1}^m p^z \sum_j (-1)^j \binom{\alpha+1}{j}\binom{r-j(p-1)-\alpha}{z} \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z} \left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right] \\ &\quad + \textstyle\sum_{m\geqslant j(p-1)+\alpha\geqslant 0} (-1)^j \binom{\alpha+1}{j} p^{j(p-1)+\alpha} \left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), x^{j(p-1)+\alpha} y^{r-j(p-1)-\alpha}\right] \\ &\quad - a \textstyle\sum_j (-1)^j \binom{1}{j} \left[1, \theta^\alpha x^{j(p-1)} y^{r-\alpha(p+1)-j(p-1)}\right] \\ &\equiv \textstyle\sum_{z=\alpha+1}^m \sum'_{j_z\in S_z} A_{j_z} p^z \left[g_{j_z}, x^z y^{r-z}\right] + p^\alpha \left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), x^\alpha y^{r-\alpha}\right] \\ &\quad - a \textstyle\sum_j (-1)^j \binom{1}{j} \left[1, \theta^\alpha x^{j(p-1)} y^{r-\alpha(p+1)-j(p-1)}\right] \pmod{p^{m+1}},\end{aligned}$$

where, for each z, the sum $\sum'_{j_z\in S_z}$ is over some finite set of indices S_z, and each A_{j_z} is a constant, and each g_{j_z} is an element of G. Note that, for each z such that $m \geqslant z \geqslant \alpha+1$, we have

$$p^z \left[g_{j_z}, x^z y^{r-z}\right] = a[g'_{j_z}, \theta^z h_{j_z}] + O(p^{m+1}) = a[g'_{j_z}, \theta^{m+1} h'_{j_z}] + O(p^{m+1}),$$

for some polynomials h_{j_z}, h'_{j_z}. It can be shown by the same algebraic manipulation used in the proof of lemma 28 that

$$\textstyle\sum_\mu p^\alpha \left[\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), x^\alpha y^{r-\alpha}\right] = \sum_{i>0} p^\alpha (p-1)\binom{r-\alpha}{i(p-1)}[1, x^{i(p-1)+\alpha} y^{r-i(p-1)-\alpha}] + O(p^{m+1}).$$

Thus, by letting

$$\tau_\dagger = p^{-\alpha}(p-1)^{-1}\left(\sum_\mu \phi^{(0)}_{\alpha+1,\alpha,\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1\end{smallmatrix}\right)} + (-1)^\alpha \delta_{L\equiv_{p-1}\alpha}\phi^{(0)}_{\alpha+1,\alpha,\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0\end{smallmatrix}\right)}\right)$$

and $a' = p^{-\alpha}(p-1)^{-1}a$, we get the equation

$$\begin{aligned}(T-a)\tau_\dagger \equiv & \sum_{i>0}\tbinom{r-\alpha}{i(p-1)}[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}] \\ & - a'\sum_j(-1)^j\tbinom{1}{j}\sum_\mu\left[\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right] \\ & - a'\sum_j(-1)^j\tbinom{1}{j}\delta_{L\equiv_{p-1}\alpha}\left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right] \\ & + a'{\sum}'_{j'\in S'} A_{j'}\left[g_{j'}, \theta^{\alpha+1}h'_{j'}\right] \pmod{p^{m+1-\alpha}}.\end{aligned}$$

Let us denote this equation by Eq. α. By adding constant multiples of expressions which are similar to Eq. 1 through Eq. $(\alpha-1)$ with $\sum_\mu$ replaced by $\sum_\mu[\mu]^l$, we can get an analogue of lemma 29:

$$\begin{aligned}(T-a)\tau_\dagger \equiv & \sum_{r-2\alpha>i(p-1)>0} D_i[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}] \\ & - a'\sum_j(-1)^j\tbinom{1}{j}\sum_\mu\left[\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right] \\ & - (-1)^{\alpha+1}\left(\sum_{l=0}^\alpha C_l\tbinom{r-\alpha+l}{\alpha}\right) \\ & \quad \times a'\sum_j(-1)^j\tbinom{1}{j}\delta_{L\equiv_{p-1}\alpha}\left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right] \\ & + a'{\sum}'_{j'\in S'} A_{j'}\left[g_{j'}, \theta^{\alpha+1}h'_{j'}\right] \pmod{p^{m+1-\alpha}},\end{aligned}$$

where $D_i = \sum_{l=0}^\alpha C_l\binom{r-\alpha+l}{i(p-1)+l}$, and $C_0 = 1$, and $v(a') = v(a) - \alpha$. We can restrict the first sum to the range $r - 2\alpha \geqslant i(p-1) > 0$ by noting that

$$[1, x^{i(p-1)+\beta}y^{r-i(p-1)-\beta}] = O(p^{m-\beta}) = O(p^{m+1-\alpha}),$$

for all β such that $\alpha > \beta \geqslant 0$. Let

$$\tau_0 = \sum_{r-2\alpha>i(p-1)>0}(c_i - D_i)\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right],$$

where

$$c_i = (-1)^{i-1}\tbinom{\alpha}{i-1}\sum_{r-2\alpha>j(p-1)>0} D_j\tbinom{j}{\alpha}.$$

We will denote by $\sum'$ the restricted sum $\sum_{r-2\alpha>i(p-1)>0}$. Then

$$\sum{}' c_i\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right] = \left(\sum{}' D_i\tbinom{i}{\alpha}\right)\left[1, \theta^\alpha x^{p-1}y^{r-(\alpha+1)(p+1)+2}\right],$$

and

$$v(c_i) \geqslant v\left(\sum_{i>0} D_i\tbinom{i}{\alpha}\right) = v\left(\sum_{i>0} c_i\tbinom{i}{\alpha}\right).$$

Finally, note that

$$\begin{aligned}(T-a)\tau_0 \equiv & \sum_{\lambda\neq 0}\sum_{z\geqslant 0} p^z\sum{}'(c_i - D_i)\tbinom{r-i(p-1)-\alpha}{z}\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), (-[\lambda])^{r-\alpha-z}x^{r-z}y^z\right] \\ & - a\sum{}'(c_i - D_i)\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right] \\ \equiv & \sum_{z=\alpha+1}^{2m+1-\alpha}\sum{}'(c_i - D_i)\tbinom{r-i(p-1)-\alpha}{z}\sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}p^z\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right] \\ & - a\sum{}'(c_i - D_i)\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right] \pmod{p^{2m+2-\alpha}}.\end{aligned}$$

Write $\mathcal{V} = v\big(\sum' D_i\binom{i}{\alpha}\big)$ and $\mathcal{V}_z = v\left(\sum'(c_i - D_i)\binom{r-i(p-1)-\alpha}{z}\right)$, and note that $\mathcal{V}_z \geqslant \mathcal{V}$, for all $\alpha < z \leqslant 2m+1-z$, by assumption. Therefore,

$$\begin{aligned}&\textstyle\sum_{z=m+1}^{2m+1-\alpha} \sum'(c_i - D_i)\binom{r-i(p-1)-\alpha}{z} \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}p^z\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right]\\ &\qquad\equiv \textstyle\sum_{z=m+1}^{2m+1-\alpha} \mathcal{V}_z p^z X_z \pmod{p^{2m+2-\alpha}},\end{aligned}$$

where X_z is some expresion such that $v(X_z) \geqslant 0$. This implies that

$$\begin{aligned}&-a^{-1}\textstyle\sum_{z=m+1}^{2m+1-\alpha} \sum'(c_i - D_i)\binom{r-i(p-1)-\alpha}{z} \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}p^z\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right]\\ &\qquad= \textstyle\sum_{z=m+1}^{2m+1-\alpha} \mathcal{V}_z X_z' + O(p^{m+1-\alpha}) = \mathcal{V}(p^{m+1-v(a)}) + O(p^{m+1-\alpha}).\end{aligned}$$

Similarly,

$$\begin{aligned}&\textstyle\sum_{z=\alpha+1}^{m} \sum'(c_i - D_i)\binom{r-i(p-1)-\alpha}{z} \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}p^z\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right]\\ &\quad= \textstyle\sum_{z=\alpha+1}^{m} \mathcal{V}_z \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}p^z\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right] + O(p^{2m+2-\alpha})\\ &\quad= \textstyle\sum_{z=\alpha+1}^{m} \mathcal{V}_z \left(\sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}a\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), \theta^z h_z\right] + O(p^{m+1})\right) + O(p^{2m+2-\alpha})\\ &\quad= \mathcal{V}\textstyle\sum_{z=\alpha+1}^{m} Y_z \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}a\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), \theta^z h_z\right] + \mathcal{V}O(p^{m+1}) + O(p^{2m+2-\alpha}),\end{aligned}$$

where h_z is some polynomial, and Y_z is some expresion such that $v(Y_z) \geqslant 0$. This implies that

$$\begin{aligned}&-a^{-1}\textstyle\sum_{z=\alpha+1}^{m} \sum'(c_i - D_i)\binom{r-i(p-1)-\alpha}{z} \sum_{\lambda\neq 0}(-[\lambda])^{r-\alpha-z}p^z\left[\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1\end{smallmatrix}\right), x^{r-z}y^z\right]\\ &\qquad= \mathcal{V}\textstyle\sum_{j\in S}[g_j, \theta^{\alpha+1}h_j'] + \mathcal{V}O(p^{m+1-v(a)}) + O(p^{m+1-\alpha}),\end{aligned}$$

where g_j is some element of G, and h_j' is some polynomial. This implies that

$$\begin{aligned}&(T-a)(\tau_\dagger - a^{-1}\tau_0)\\ &\quad\equiv \textstyle\sum' c_i\left[1, x^{i(p-1)+\alpha}y^{r-i(p-1)-\alpha}\right] + \mathcal{V}\sum_{j\in S}[g_j, \theta^{\alpha+1}h_j'] + \mathcal{V}O(p^\delta)\\ &\qquad - a'\textstyle\sum_j(-1)^j\binom{1}{j}\sum_\mu\left[\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right]\\ &\qquad - (-1)^{\alpha+1}\left(\textstyle\sum_{l=0}^{\alpha} C_l\binom{r-\alpha+l}{\alpha}\right)\\ &\qquad\qquad \times a'\textstyle\sum_j(-1)^j\binom{1}{j}\delta_{L\equiv_{p-1}\alpha}\left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right]\\ &\qquad + a'\textstyle\sum_{j'\in S'}' A_{j'}\left[g_{j'}, \theta^{\alpha+1}h_{j'}'\right]\\ &\quad\equiv \left(\textstyle\sum' D_i\binom{i}{\alpha}\right)\left[1, \theta^\alpha x^{p-1}y^{r-(\alpha+1)(p+1)+2}\right] + \mathcal{V}\sum_{j\in S}[g_j, \theta^{\alpha+1}h_j'] + \mathcal{V}O(p^\delta)\\ &\qquad - a'\textstyle\sum_j(-1)^j\binom{1}{j}\sum_\mu\left[\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1\end{smallmatrix}\right), \theta^\alpha x^{j(p-1)}y^{r-\alpha(p+1)-j(p-1)}\right]\\ &\qquad - (-1)^{\alpha+1}\left(\textstyle\sum_{l=0}^{\alpha} C_l\binom{r-\alpha+l}{\alpha}\right)\\ &\qquad\qquad \times a'\textstyle\sum_j(-1)^j\binom{1}{j}\delta_{L\equiv_{p-1}\alpha}\left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right), \theta^\alpha y^{j(p-1)}x^{r-\alpha(p+1)-j(p-1)}\right]\\ &\qquad + a'\textstyle\sum_{j'\in S'}' A_{j'}\left[g_{j'}, \theta^{\alpha+1}h_{j'}'\right] \pmod{p^{m+1-\alpha}},\end{aligned}$$

where $\delta = m+1-\alpha > 0$. If $\mathfrak{v}_\alpha(C_1, \ldots, C_\alpha) < v(a) - \alpha$, then

$$\Psi_\alpha\left(\overline{(T-a)(\mathfrak{m}_\alpha(C_1, \ldots, C_\alpha))^{-1}(\tau_\dagger - a^{-1}\tau_0)}\right) = [1, X^{(2\alpha - r \bmod p-1)}]$$

is in the image under Ψ_α of the kernel of reduction, and generates $I(\sigma_{(2\alpha-r \bmod p-1)}(r-\alpha))$. If, on the other hand, $\mathfrak{v}_\alpha(C_1, \ldots, C_\alpha) > v(a) - \alpha$, then

$$\Psi_\alpha\left(\overline{(T-a)(a')^{-1}(\tau_\dagger - a^{-1}\tau_0)}\right) = T[1, X^{(2\alpha - r \bmod p-1)}]$$

is in the image under Ψ_α of the kernel of reduction, and generates $T\left(I(\sigma_{(2\alpha-r \bmod p-1)}(r-\alpha))\right)$. ∎

Remark. In the statement of theorem 27, we can replace the binomials $\binom{i}{w}$ by $f_w(i)$, where f_w is any polynomial of degree w whose top coefficient is a unit in $\mathbb{Z}_p$. This can be proved by a simple application of row operations.

4 The case when $v(a) = 1$

4.1 The main theorem

We follow the approach outlined in [14, 15]. The main result in this section is theorem 31.

Theorem 31. *Let $t \geqslant 1$ be an integer, and let $r = t(p-1) + s$, with $s \in \{2, \ldots, p-1\}$. Let $a \in \overline{\mathbb{Q}}_p$ be such that $v(a) = 1$. Then, for any*

$$\gamma \in \left(T - \overline{p/a} \cdot \tfrac{t}{s}\right)(I(\sigma_{p-1-s}(s))),$$

there is a τ such that $(T-a)\tau$ and $p^2\tau$ are integral, and $\Psi(\overline{(T-a)\tau}) = \gamma$.

Before giving the proof of theorem 31, we will first prove a lemma.

4.2 A lemma

Lemma 32. *Let $t \geqslant 1$ be an integer, and let $a \in \overline{\mathbb{Q}}_p$ be such that $v(a) = 1$. Let $r = t(p-1)+s$, with $s \in \{2, \ldots, p-1\}$. Then there is some τ such that $(T-a)\tau$ and $p^2\tau$ are integral, and*

$$\Psi(\overline{(T-a)\tau}) = \left(T - \overline{p/a} \cdot \tfrac{t}{s}\right)\left[1, X^{p-1-s}\right].$$

Proof. Let $l \in \{1, \ldots, t\}$, and let $\varphi_{l,g} = \left[g, y^r - x^{l(p-1)}y^{r-l(p-1)}\right]$. Then

$$\begin{aligned}(T-a)\varphi_{l,g} \equiv \textstyle\sum_{\lambda \neq 0} &\left[g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), \left\{(-[\lambda])^r - (-[\lambda])^{r-l(p-1)}\right\} x^r\right. \\ &+ \left.\left\{r(-[\lambda])^{r-1} - (r - l(p-1))(-[\lambda])^{r-l(p-1)-1}\right\} px^{r-1}y\right] \\ &+ \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), y^r\right] - \left[g, a(y^r - x^{l(p-1)}y^{r-l(p-1)})\right] \pmod{p^2},\end{aligned}$$

Note that, for $\lambda \neq 0$, $(-[\lambda])^r = (-[\lambda])^{r-l(p-1)}$ and $(-[\lambda])^{r-1} = (-[\lambda])^{r-l(p-1)-1} = (-[\lambda])^{s-1}$. Hence

$$\begin{aligned}(T-a)\varphi_{l,g} \equiv \textstyle\sum_{\lambda \neq 0} &\left[g\left(\begin{smallmatrix} p & [\lambda] \\ 0 & 1 \end{smallmatrix}\right), (-[\lambda])^{s-1} lp(p-1)x^{r-1}y\right] \\ &+ \left[g\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), y^r\right] - \left[g, a(y^r - x^{l(p-1)}y^{r-l(p-1)})\right] \pmod{p^2}.\end{aligned}$$

Let $\tau' = \sum_{\mu \in \mathbb{F}_p} \varphi_{l,\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right)}$. Then

$$\begin{aligned}(T-a)\tau' \equiv -pl \textstyle\sum_{\lambda \neq 0, \mu} &\left[\left(\begin{smallmatrix} p^2 & p[\lambda]+[\mu] \\ 0 & 1 \end{smallmatrix}\right), (-[\lambda])^{s-1}x^{r-1}y\right] + \textstyle\sum_\mu \left[\left(\begin{smallmatrix} 1 & [\mu] \\ 0 & 1 \end{smallmatrix}\right), y^r\right] \\ &- \textstyle\sum_\mu a\left[\left(\begin{smallmatrix} p & [\mu] \\ 0 & 1 \end{smallmatrix}\right), y^r - x^{l(p-1)}y^{r-l(p-1)}\right] \pmod{p^2}.\end{aligned}$$

Note that

$$\textstyle\sum_\mu \left[\left(\begin{smallmatrix} 1 & [\mu] \\ 0 & 1 \end{smallmatrix}\right), y^r\right] \equiv \sum_\mu \left[1, (y + [\mu]x)^r\right] \equiv \sum_{i,\mu} \binom{r}{i}[\mu]^i \left[1, x^i y^{r-i}\right] \pmod{p^2},$$

and that $\sum_\mu [\mu]^i = 0$ if $i \notin \{0, p-1, \ldots, t(p-1), (t+1)(p-1)\}$, and $\sum_\mu [\mu]^i = p - 1 + \delta_{i=0}$

otherwise. Consequently,

$$\begin{aligned}\textstyle\sum_\mu [\left(\begin{smallmatrix}1 & [\mu]\\ 0 & 1\end{smallmatrix}\right), y^r] \equiv p\binom{r}{0}[1, y^r] &+ (p-1)\delta_{s=p-1}\tbinom{r}{(t+1)(p-1)}[1, x^r] \\ &+ (p-1)\textstyle\sum_{j=1}^t \binom{r}{j(p-1)}\left[1, x^{j(p-1)}y^{r-j(p-1)}\right] \pmod{p^2},\end{aligned}$$

which implies that

$$\begin{aligned}(T-a)\tau' \equiv -lp\textstyle\sum_{\lambda\neq 0,\mu}&\left[\left(\begin{smallmatrix}p^2 & p[\lambda]+[\mu]\\ 0 & 1\end{smallmatrix}\right), (-[\lambda])^{s-1}x^{r-1}y\right] \\ &+ p(p-1)\textstyle\sum_{j=1}^t p^{-1}\binom{r}{j(p-1)}\left[1, x^{j(p-1)}y^{r-j(p-1)}\right] + p[1, y^r] \\ &+ (p-1)\delta_{s=p-1}[1, x^r] - p\textstyle\sum_\mu \frac{a}{p}\left[\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right), y^r - x^{l(p-1)}y^{r-l(p-1)}\right] \pmod{p^2}.\end{aligned}$$

Note also that

$$\begin{aligned}(T-a)\varphi_{l,\left(\begin{smallmatrix}0 & 1\\ p & 0\end{smallmatrix}\right)} &\equiv \textstyle\sum_{\lambda\neq 0}\left[\left(\begin{smallmatrix}0 & 1\\ p^2 & p[\lambda]+1\end{smallmatrix}\right), (-[\lambda])^{-1}lp(p-1)x^{r-1}y\right] \\ &\quad + [\left(\begin{smallmatrix}0 & p\\ p & 0\end{smallmatrix}\right), y^r] - a\left[\left(\begin{smallmatrix}0 & 1\\ p & 0\end{smallmatrix}\right), y^r - x^{l(p-1)}y^{r-l(p-1)}\right] \\ &\equiv \textstyle\sum_{\lambda\neq 0}\left[\left(\begin{smallmatrix}0 & 1\\ p^2 & p[\lambda]+1\end{smallmatrix}\right), (-[\lambda])^{-1}lp(p-1)x^{r-1}y\right] \\ &\quad + [1, x^r] - a\left[\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), x^r - y^{l(p-1)}x^{r-l(p-1)}\right] \pmod{p^2}.\end{aligned}$$

Let $\tau'' = \tau' + \delta_{s=p-1}\varphi_{l,\left(\begin{smallmatrix}0 & 1\\ p & 0\end{smallmatrix}\right)}$, so that τ'' is integral. Then

$$\begin{aligned}(T-a)\tau'' \equiv -lp\textstyle\sum_{\lambda\neq 0,\mu}&\left[\left(\begin{smallmatrix}p^2 & p[\lambda]+[\mu]\\ 0 & 1\end{smallmatrix}\right), (-[\lambda])^{s-1}x^{r-1}y\right] + p[1, y^r] + p\delta_{s=p-1}[1, x^r] \\ &+ p(p-1)\textstyle\sum_{j=1}^t p^{-1}\binom{r}{j(p-1)}\left[1, x^{j(p-1)}y^{r-j(p-1)}\right] \\ &- p\textstyle\sum_\mu \frac{a}{p}\left[\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right), y^r - x^{l(p-1)}y^{r-l(p-1)}\right] \\ &+ p\delta_{s=p-1}\textstyle\sum_{\lambda\neq 0}\left[\left(\begin{smallmatrix}0 & 1\\ p^2 & p[\lambda]+1\end{smallmatrix}\right), (-[\lambda])^{-1}l(p-1)x^{r-1}y\right] \\ &- p\delta_{s=p-1}\frac{a}{p}\left[\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), x^r - y^{l(p-1)}x^{r-l(p-1)}\right] \pmod{p^2}.\end{aligned}$$

Let $\tau''' = \frac{p}{a}\sum_{j=1}^t b_j\varphi_{j,1}$, where $b_j \in \mathbb{Q}_p$ are such that $pb_j \in \mathbb{Z}_p$ and $\sum_{j=1}^t b_j = 0$. Then $p\tau'''$ is integral, and

$$\begin{aligned}(T-a)\tau''' \equiv -\textstyle\sum_{\lambda\neq 0} p\left(\sum_{j=1}^t jb_j\right)&\left[\left(\begin{smallmatrix}p & [\lambda]\\ 0 & 1\end{smallmatrix}\right), (-[\lambda])^{s-1}\frac{p}{a}x^{r-1}y\right] \\ &+ p\textstyle\sum_{j=1}^t b_j\left[1, x^{j(p-1)}y^{r-j(p-1)}\right] \pmod{p^2}.\end{aligned}$$

In particular, this equation holds true when $b_j = c_j - p^{-1}\binom{r}{j(p-1)}$, where $c_j \in \mathbb{Z}_p$ are such that $\sum_{j=1}^t c_j = \frac{t}{s}$. Consequently, if

$$\tau'''' = \tau'' + \tau''' = \textstyle\sum_{\mu\in\mathbb{F}_p}\varphi_{l,\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right)} + \delta_{s=p-1}\varphi_{l,\left(\begin{smallmatrix}0 & 1\\ p & 0\end{smallmatrix}\right)} + \frac{p}{a}\sum_{j=1}^t\left(c_j - p^{-1}\binom{r}{j(p-1)}\right)\varphi_{j,1},$$

then $p\tau''''$ is integral, and

$$\begin{aligned}(T-a)\tau'''' \equiv -lp\textstyle\sum_{\lambda\neq 0,\mu}&\left[\left(\begin{smallmatrix}p^2 & p[\lambda]+[\mu]\\ 0 & 1\end{smallmatrix}\right), (-[\lambda])^{s-1}x^{r-1}y\right] + p[1, y^r] + p\delta_{s=p-1}[1, x^r] \\ &+ p\delta_{s=p-1}\textstyle\sum_{\lambda\neq 0}\left[\left(\begin{smallmatrix}0 & 1\\ p^2 & p[\lambda]+1\end{smallmatrix}\right), (-[\lambda])^{-1}l(p-1)x^{r-1}y\right] \\ &- \textstyle\sum_{\lambda\neq 0} p\left(\sum_{j=1}^t j\left(c_j - p^{-1}\binom{r}{j(p-1)}\right)\right)\left[\left(\begin{smallmatrix}p & [\lambda]\\ 0 & 1\end{smallmatrix}\right), (-[\lambda])^{s-1}\frac{p}{a}x^{r-1}y\right] \\ &+ p(p-1)\textstyle\sum_{j=1}^t c_j\left[1, x^{j(p-1)}y^{r-j(p-1)}\right] - p\sum_\mu \frac{a}{p}\left[\left(\begin{smallmatrix}p & [\mu]\\ 0 & 1\end{smallmatrix}\right), y^r - x^{l(p-1)}y^{r-l(p-1)}\right] \\ &- p\delta_{s=p-1}\frac{a}{p}\left[\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right), x^r - y^{l(p-1)}x^{r-l(p-1)}\right] \pmod{p^2}.\end{aligned}$$

Note that

$$v\left(\textstyle\sum_{j=1}^t j\left(c_j - p^{-1}\binom{r}{j(p-1)}\right)\right) \geqslant 0,$$

due to lemma 21. Let $\tau = a^{-1}\tau''''$. Then $(T-a)\tau$ and $p^2\tau$ are integral. Moreover, $\Psi y^r = 0$ and $\Psi x^{r-1}y = 0$, since $s \neq 1$. Consequently,

$$\Psi(\overline{(T-a)\tau}) = \left(T - \overline{p/a}\sum_{j=1}^{t} c_j\right)\left[1, X^{p-1-s}\right] = \left(T - \overline{p/a}\cdot\tfrac{t}{s}\right)\left[1, X^{p-1-s}\right].$$

□

Proof of theorem 31. Follows from lemma 32 due to the fact that the module $\sigma_{p-1-s}(s)$ is simple and hence generated by X^{p-1-s}. □

4.3 Completing the proof of theorem 4

Lemma 33. *Let $t \geqslant 2$ be an integer, and let $a \in \overline{\mathbb{Q}}_p$ be such that $v(a) = 1$. Suppose that $r = t(p-1)+s$, with $s \in \{2,4,\ldots,p-1\}$. If $p \nmid t$, then $\overline{\Theta}_{r+2,a}$ is one of the following:*

— *either $\overline{\Theta}_{r+2,a}^{\mathrm{ss}} \cong \pi(\widetilde{s-2},\lambda,\omega)^{\mathrm{ss}} \oplus \pi(p-1-s,\lambda^{-1},\omega^s)^{\mathrm{ss}}$, where $\lambda = \overline{a/p}\cdot\frac{s}{t}$, and $\widetilde{n}$ is the integer in $\{1,\ldots,p-1\}$ which is congruent to n modulo $p-1$; or $\overline{\Theta}_{r+2,a} \cong \pi(s-2,0,\omega)$.*

If, on the other hand, $p \mid t$, then $\overline{\Theta}_{r+2,a}$ is one of the following:

— *either $\overline{\Theta}_{r+2,a} \cong \pi(s,0,1)$; or $\overline{\Theta}_{r+2,a} \cong \pi(s-2,0,\omega)$.*

Proof. First, we will consider the case when $r \neq 2p$. A consequence of lemma 14, with $A = I(\sigma_r)$, with $B = I(\sigma^{p-1-s}(s))$, with β being induced by Ψ, with $B' = \left(T - \overline{p/a}\cdot\frac{t}{s}\right)(I(\sigma_{p-1-s}(s)))$, with $C = \overline{\Theta}_{r+2,a}$, and with γ being the surjection $\sigma_r \twoheadrightarrow \overline{\Theta}_{r+2,a}$, is the fact that there is some $C_1 \subseteq \overline{\Theta}_{r+2,a}$ such that $\overline{\Theta}_{r+2,a}/C_1$ is isomorphic to a quotient of $I(\sigma_{p-1-s}(s))/B'$ and C_1 is isomorphic to $I(\ker\Psi)/(I(\ker\Psi)\cap X(r+2,a))$. Here the choice of B' can be made due to theorem 31. Firstly, suppose that $p \nmid t$. Note that $I(\sigma_{p-1-s}(s))/\left(T - \overline{p/a}\cdot\frac{t}{s}\right) \cong \pi(p-1-s,\lambda^{-1},\omega^s)$, where $\lambda = \overline{a/p}\cdot\frac{s}{t}$. Hence, $\overline{\Theta}_{r+2,a}$ is a quotient of a module which has a series with factors

$$\pi(p-1-s,\lambda^{-1},\omega^s),\ I\left(\langle\overline{\theta}\sigma_{r-(p+1)}, y^r\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}\right) \big/ \left(I\left(\langle\overline{\theta}\sigma_{r-(p+1)}, y^r\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}\right)\cap X(r+2,a)\right).$$

Since $X(r+2,a)$ contains $I(Y_r)$, due to lemma 15, this is a quotient of a module which has a series with factors

$$\pi(p-1-s,\lambda^{-1},\omega^s),\ I\left(\langle\overline{\theta}\sigma_{r-(p+1)}, y^r\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}/\langle\overline{\theta}^2\sigma_{r-2(p+1)}, y^r\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}\right).$$

It can be shown, by several applications of the isomorphism theorems, that

$$\langle\overline{\theta}\sigma_{r-(p+1)}, y^r\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}/\langle\overline{\theta}^2\sigma_{r-2(p+1)}, y^r\rangle_{\mathrm{GL}_2(\mathbb{F}_p)}$$

is a quotient of $M = \overline{\theta}\sigma_{r-(p+1)}/\overline{\theta}^2\sigma_{r-2(p+1)}$. Due to parts (a) and (c) of lemma 3.2 in [1], there is a series $M = M_2 \supseteq M_1 \supseteq M_0 = \{0\}$, such that M_2/M_1 is isomorphic to $\sigma_{(2-s \bmod p-1)}(s-1)$, and M_1 is isomorphic to $\sigma_{\widetilde{s-2}}(1)$, where $\widetilde{n}$ is the integer in $\{1,\ldots,p-1\}$ which is congruent to n modulo $p-1$. Hence $\overline{\Theta}_{r+2,a}$ is a quotient of a module which has a series with factors

$$\pi(p-1-s,\lambda^{-1},\omega^s),\ I\left(\sigma_{(2-s \bmod p-1)}(s-1)\right),\ I\left(\sigma_{\widetilde{s-2}}(1)\right).$$

If $s \notin \{1,2,3\}$, the only pair of integers from the set $\{p-1-s, \widetilde{s-2}, (2-s \bmod p-1)\}$ which adds up to $(-2 \bmod p-1)$ is the pair $(p-1-s, \widetilde{s-2})$, since $p \geqslant 5$. If $s=2$ and $p \geqslant 5$, then there are also the pairs $(p-3,0)$ and $(p-3,p-1)$, which can't give a reducible representation since $\omega \neq \omega^{p-1}$. If $p=3$ and $s=2$, then it can't be the case that $\overline{\Theta}_{r+2,a}^{\mathrm{ss}} \cong \pi(\nu,\lambda,\omega)^{\mathrm{ss}} \oplus \pi(0,\lambda^{-1},\omega)^{\mathrm{ss}}$ with $\nu \in \{0,2\}$, since $\omega \neq \omega^{\nu+2}$. Consequently, due to the classification in theorem 2, either $\overline{\Theta}_{r+2,a}^{\mathrm{ss}} \cong \pi(\widetilde{s-2},\lambda,\omega)^{\mathrm{ss}} \oplus \pi(p-1-s,\lambda^{-1},\omega^s)^{\mathrm{ss}}$, or $\overline{\Theta}_{r+2,a} \cong \pi(\widetilde{s-2},0,\omega)$.

Now suppose that $p \mid t$. Then, similarly, $\overline{\Theta}_{r+2,a}$ is a quotient of a module which has a series with factors

$$\pi(s,0,1),\ I\left(\sigma_{(2-s \bmod p-1)}(s-1)\right),\ I\left(\sigma_{\widetilde{s-2}}(1)\right).$$

Then $\overline{\Theta}_{r+2,a}$ must be irreducible, since if $p \geqslant 5$ and $s \notin \{1,3\}$, then there is no pair of integers from the set $\{\widetilde{s-2}, (2-s \bmod p-1)\}$ which adds up to $(-2 \bmod p-1)$, and if $p=3$ and $s \notin \{1,3\}$, then it can't be the case that $\overline{\Theta}^{\mathrm{ss}}_{r+2,a} \cong \pi(\nu,\lambda,\omega)^{\mathrm{ss}} \oplus \pi(0,\lambda^{-1},\omega)^{\mathrm{ss}}$ with $\nu \in \{0,2\}$, since $\omega \neq \omega^{\nu+2}$. Consequently, due to the classification in theorem 2, either $\overline{\Theta}_{r+2,a} \cong \pi(s,0,1)$, or $\overline{\Theta}_{r+2,a} \cong \pi(\widetilde{s-2},0,\omega)$.

Finally, if $r=2p$, then theorem 31 and the first part of this proof still apply, the only difference being that the second to last factor in the series for $\overline{\Theta}_{r+2,a}$ does not occur, so that $\overline{\Theta}_{r+2,a}$ is a quotient of a module which has a series with factors

$$\pi(p-1-s,\lambda^{-1},\omega^s),\ I\left(\sigma_{\widetilde{s-2}}(1)\right).$$

This completes the proof of lemma 33. □

Proof of theorem 4. Follows from theorem 2, lemma 33, and previously known results in the case when $r \leqslant 2p-2$. □

5 Conjecture 3

5.1 The case when $2 > v(a) > 1$

In this subsection, we will complete the proof of theorem 5.

Proof of theorem 5. — *The case when $s \neq 2$.* The condition that $s \neq 2$ implies that $p \geqslant 5$ and $s \in \{4,\dots,p-1\}$. Then $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-1-s}(s)\right),\ I\left(\sigma_{p+1-s}(s-1)\right),\ I\left(\sigma_{s-2}(1)\right).$$

Due to the conditions $p \geqslant 5$ and $s \in \{4,\dots,p-1\}$, the only pair of factors which can give a reducible $\overline{\Theta}_{r+2,a}$ is $(I\left(\sigma_{p-1-s}(s)\right), I\left(\sigma_{s-2}(1)\right))$. Let $\alpha=0$, and define M_r by the equation $M_r = \sum_{r>j(p-1)>0} \binom{r}{j(p-1)}$. Then, in view of lemma 21, we have $\mathfrak{m}_0(\varnothing) = M_r$, so

$$v(\mathfrak{m}_0(\varnothing)) = v(\tfrac{t}{s}p(1+O(p))) = v(t).$$

Moreover, $v(\mathfrak{m}_w(\varnothing))$ can be expressed as a linear combination of $M_r, M_{r-1}, \dots, M_{r-w}$. In particular, since $s>3$, it follows that $v(M_{r-i}) = v(t)$, for all $i \in \{0,1,2,3\}$, which implies that $v(\mathfrak{m}_0(\varnothing)) \geqslant v(\mathfrak{m}_w(\varnothing))$, for all $w \in \{1,2,3\}$. Consequently, theorem 27 can be applied to show that either $[1, X^{p+1-s}]$ is in the image under Ψ_1 of the kernel of reduction, or $T[1, X^{p+1-s}]$ is in the image under Ψ_1 of the kernel of reduction. In any case, $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p+1-s}(s-1)\right),\ I\left(\sigma_{s-2}(1)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$, which completes the proof in the case $s \neq 2$.

— *The case when $s=2$ and $t \not\equiv \{1,2\}$* (mod p). The matrix $\mathfrak{M}^{(r,1,1)}$ contains

$$\mathfrak{M}' = \begin{pmatrix} 1 & 1 & \sum_{r-3>i(p-1)>0} \binom{r}{i(p-1)+1} \\ 1-r & 1 & \sum_{r-3>i(p-1)>0} \binom{r}{i(p-1)+1} i \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2(1-r) \\ 1-r & 1 & (1-r)(2-r) \end{pmatrix}$$

as a submatrix, which has full rank over $\mathbb{F}_p$ (and therefore contains $(0,1)^T$ in its range) for $r \not\equiv 0 \pmod p$. Moreover, if v_1, v_2, v_3 denote the columns of $\mathfrak{M}'$, then

$$(r-1)v_1 + (r-1)v_2 + v_3 = 0,$$

so there is an element $\nu \in \overline{\theta}\sigma_{r-(p+1)}$ in the subspace $N \subseteq \overline{\theta}\sigma_{r-(p+1)}$ which corresponds to σ_{p-1}, such that the coefficient of $\overline{\theta}x^{r-(p-1)}$ in ν is $r-1$. Consequently, if $r \not\equiv 1 \pmod p$, then this element does not belong to $\overline{\theta}^2\sigma_{r-2(p+1)}$. Therefore, unless $p \mid r(r-1)$, we have that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p+1-s}(s-1)\right), I\left(\sigma_{s-2}(1)\right),$$

which cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$. This completes the proof in the case when $s = 2$ and $t \not\equiv \{1,2\} \pmod p$.

— *The case when $s = 2$ and $t \equiv \{1,2\}$* $\pmod p$. Calling the method `find_m_w(1,0,1)` in the second program in the appendix shows that in both cases the relevant $\mathfrak{m}_w(\varnothing)$ are either zero or polynomials of the type $Cr^\alpha(r-1)^\beta$. More specifically,

$$\begin{aligned}\mathfrak{m}_2(\varnothing) &= \tfrac{1}{2}r(r-1),\\ \mathfrak{m}_3(\varnothing) &= -\tfrac{1}{2}r^2(r-1).\end{aligned}$$

In particular, if $t \equiv \{1,2\} \pmod p$ then all of the relevant $\mathfrak{m}_w(\varnothing)$ vanish. So theorem 27 applies, and shows that the factor which is a quotient of $I\left(\sigma_{p-3}(2)\right)$ is in fact a quotient of $\pi(p-3, 0, \omega^2)$, which implies that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of $I\left(\sigma_{p+1-s}(s-1)\right), I\left(\sigma_{s-2}(1)\right)$, which cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$. Consequently, $\overline{\Theta}_{r+2,a}$ must be irreducible. This completes the proof in the case when $s = 2$ and $t \equiv \{1,2\} \pmod p$.

□

5.2 The case when $3 > v(a) > 2$

In this subsection, we will complete the proof of theorem 6.

Proof of theorem 6. The case when $p = 3$ is vacuous, so in the remainder of this proof we are going to assume that $p > 3$.

— *The case when $s \notin \{2,4\}$ and $t \not\equiv \{0,1\}$* $\pmod p$. The condition that $s \notin \{2,4\}$ implies that $p \geqslant 7$ and $s \in \{6, \dots, p-1\}$, and theorem 27 applies. Then $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-1-s}(s)\right), I\left(\sigma_{p+1-s}(s-1)\right), I\left(\sigma_{s-2}(1)\right), I\left(\sigma_{p+3-s}(s-2)\right), I\left(\sigma_{s-4}(2)\right).$$

Due to the conditions $p \geqslant 7$ and $s \in \{6, \dots, p-1\}$, the only pairs of factors which can give a reducible $\overline{\Theta}_{r+2,a}$ are

$$\left(I\left(\sigma_{p-1-s}(s)\right), I\left(\sigma_{s-2}(1)\right)\right), \left(I\left(\sigma_{p+1-s}(s-1)\right), I\left(\sigma_{s-4}(2)\right)\right).$$

Now, suppose that $t \notin \{0,1\}$. For $\alpha = 1$, after choosing the constant $C_1 = -\frac{p}{s-1} + O(p^2)$ in theorem 27, where $O(p^2)$ is such that $\mathfrak{m}_0(C_1) = 0$, we have $v(\mathfrak{m}_w(C_1)) \geqslant 1$ for $w \in \{1,2,3,4\}$, and

$$\mathfrak{m}_1(C_1) = \textstyle\sum_{i>0}\sum_{l=0}^{\alpha} C_l \binom{r-1+l}{i(p-1)+l} i = \frac{pt(r-1)}{(s-1)(s-2)} - \frac{pt}{s-1} = \frac{pt(1-t)}{(s-1)(s-2)},$$

so $v(\mathfrak{m}_1(C_1)) = 1$. Consequently, theorem 27 can be applied to show that $[1, X^{p+1-s}]$ is

in the image under Ψ_1 of the kernel of reduction. Since $I_{s-2}(1)$ is not semi-simple, due to lemma 19, $[1, X^{p+1-s}]$ generates the whole of $I_{s-2}(1)$, which implies that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-1-s}(s)\right), \, I\left(\sigma_{p+3-s}(s-2)\right), \, I\left(\sigma_{s-4}(2)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$, which completes the proof in the case $t \not\equiv \{0,1\} \pmod p$.

— *The case when* $s \notin \{2,4\}$ *and* $t \equiv 1 \pmod p$. Due to the remark succeeding the proof of theorem 27, we can replace the binomials $\binom{i}{w}$ in the statement of the theorem by $\binom{i(p-1)}{w}$. Then we have $v(\mathfrak{m}_1(C_1)) \geqslant 2$. Moreover, $v(C_1) \geqslant 1$, and

$$\begin{aligned}
v & \left((-1)^{w+1} + \textstyle\sum_{i>0} \binom{r}{i(p-1)+1}\binom{i(p-1)}{w}\right) \\
&= v\left((-1)^{w+1} + O(p) + \textstyle\sum_{i>0} \binom{r}{i(p-1)+1} \sum_v (-1)^{w-v}\binom{i(p-1)+1}{v}\right) \\
&= v\left((-1)^{w+1} + O(p) + \textstyle\sum_v \sum_{i>0} \binom{r-v}{i(p-1)+1-v}(-1)^{w-v}\binom{r}{v}\right) \\
&= v\left(O(p) + \textstyle\sum_{v>0} \sum_{i>0} \binom{r-v}{i(p-1)+1-v}(-1)^{w-v}\binom{r}{v}\right) \geqslant 1.
\end{aligned}$$

The last part follows since $v\left(\sum_{i>0} \binom{r-v}{i(p-1)+1-v}\right) \geqslant 1$, whenever $v > 0$, by lemma 25. So we find, by lemmas 21 and 23, that

$$\begin{aligned}
\mathfrak{m}_w(C_1) &= \textstyle\sum_{i>0} \sum_{l=0}^{1} C_l \binom{r-1+l}{i(p-1)+l}\binom{i(p-1)}{w} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + \textstyle\sum_{i>0} \binom{r-1}{i(p-1)}\binom{i(p-1)}{w} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + \binom{r-1}{w} \textstyle\sum_{i>0} \binom{r-1-w}{i(p-1)-w} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + \binom{r-1}{w} \textstyle\sum_{i>0} \sum_v (-1)^v \binom{w}{v}\binom{r-1-v}{i(p-1)} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + p\binom{r-1}{w} \textstyle\sum_v (-1)^v \binom{w}{v} \frac{1}{s-1-v} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + p\binom{r-1}{w}(-1)^w \tfrac{w!}{(s-1)_{w+1}} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + (-1)^w p \tfrac{(r-1)_w}{(s-1)_{w+1}} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + (-1)^w p \tfrac{(s-2)_w}{(s-1)_{w+1}} \\
&= O(p^2) - (-1)^w \tfrac{p}{s-1} + (-1)^w \tfrac{p}{s-1} = O(p^2),
\end{aligned}$$

for $w \in \{1,2,3,4\}$. Consequently, theorem 27 can be applied to show that $[1, X^{p+1-s}]$ is in the image under Ψ_1 of the kernel of reduction. Similarly, when $\alpha = 0$, we have $v(\mathfrak{m}_w(\varnothing)) \geqslant 1$ for $w \in \{0,1,2,3,4,5\}$, with equality for $w = 0$ since $\mathfrak{m}_0(\varnothing) = \frac{t}{s}p + O(p^2)$. So theorem 27 can be applied to show that $[1, X^{p-1-s}]$ is in the image under Ψ_0 of the kernel of reduction. This implies that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{s-2}(1)\right), \, I\left(\sigma_{p+3-s}(s-2)\right), \, I\left(\sigma_{s-4}(2)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$, which completes the proof in the case $t \equiv 1 \pmod p$.

— *The case when* $s \notin \{2,4\}$ *and* $t \equiv 0 \pmod p$. A similar calculation to the one in the previous paragraph shows that, for $\alpha = 1$ and $w \in \{0,1,2,3,4\}$, we have $v(\mathfrak{m}_w(C_1)) \geqslant 2$, so theorem 27 can be applied to show that $T[1, X^{p+1-s}]$ is in the image under Ψ_1 of the kernel of reduction. For $\alpha = 0$ and $w \in \{0,1,2,3,4,5\}$, a similar calculation shows that $v(\mathfrak{m}_w(\varnothing)) \geqslant 2$. Suppose we define M_r by the equation $M_r = \sum_{r>j(p-1)>0} \binom{r}{j(p-1)}$. Then, in view of lemma 21, we have $\mathfrak{m}_0(\varnothing) = M_r$, so

$$v(\mathfrak{m}_0(\varnothing)) = v(\tfrac{t}{s}p(1 + O(p))) = v(t).$$

Moreover, $v(\mathfrak{m}_w(\varnothing))$ can be expressed as a linear combination of $M_r, M_{r-1}, \ldots, M_{r-w}$. In particular, since $s > 5$, it follows that $v(M_{r-i}) = v(t)$, for all $i \in \{0,1,2,3,4,5\}$, which implies that $v(\mathfrak{m}_0(\varnothing)) \geqslant v(\mathfrak{m}_w(\varnothing))$, for all $w \in \{1,2,3,4,5\}$. Therefore, if $v(\mathfrak{m}_0(\varnothing)) \geqslant 3$, then $v(\mathfrak{m}_w(\varnothing)) \geqslant 3$ for $w \in \{1,2,3,4,5\}$, and then the proof of the case when $t \equiv 0 \pmod p$ can be completed in the same fashion as the proof of the case $t \equiv 1 \pmod p$.

— *The case when $s = 2$ and $r \not\equiv \{0,1\} \pmod p$.* In this case,

$$\overline{(T-a)(p^{-2}\phi^*_{r,2,3,2,\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)})} = [1, x^2 y^{r-2}]$$

gets mapped to $[1, Y^{p-3}]$ by Ψ_0. Consequently, theorem 27 can be applied to show that $[1, Y^{p-3}]$ is in the image under Ψ_0 of the kernel of reduction. Moreover, the matrix $\mathfrak{M}^{(r,2,1)}$ contains

$$\mathfrak{M}' = \begin{pmatrix} 1 & 1 & \sum_{r-3>i(p-1)>0} \binom{r}{i(p-1)+1} \\ 1-r & 1 & \sum_{r-3>i(p-1)>0} \binom{r}{i(p-1)+1} i \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2(1-r) \\ 1-r & 1 & (1-r)(2-r) \end{pmatrix}$$

as a submatrix, which has full rank over $\mathbb{F}_p$ (and therefore contains $(0,1)^T$ in its range) for $r \not\equiv 0 \pmod p$. Moreover, if v_1, v_2, v_3 denote the columns of $\mathfrak{M}'$, then

$$(r-1)v_1 + (r-1)v_2 + v_3 = 0.$$

Therefore, there is an element $\nu \in \overline{\theta}\sigma_{r-(p+1)}$ which belongs to the subspace $N \subseteq \overline{\theta}\sigma_{r-(p+1)}$ corresponding to σ_{p-1}, such that the coefficient of $\overline{\theta}x^{r-(p-1)}$ in ν is $r-1$. Consequently, if $r \not\equiv 1 \pmod p$, then this element does not belong to $\overline{\theta}^2\sigma_{r-2(p+1)}$. This means that, unless $p \mid r(r-1)$, we have that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I(\sigma_2),\ I(\sigma_{p-3}(2)),$$

which cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$. This completes the proof in the case when $s = 2$.

Calculating the determinants of the relevant square submatrices of $\mathfrak{M}^{(r,m,\alpha)}$ is completely automated by the first program written in `Sage` listed in the appendix. In particular, calling the method `print_the_roots_for_all_matrices(m,True)` with `m` $= x$ lists the possible congruence classes modulo $p(p-1)$ outside of which $\overline{\Theta}_{r+2,a}$ is irreducible, when $m = x$ and $s \in \{2, \ldots, 2x\}$.

— *The case when $s = 2$ and $r \equiv 0 \pmod p$.* By calling the methods `exceptional_cases(2,1,1)` and `gcd_for_the_matrix(2,1,1)`, we can show that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I(\sigma_0(1)),\ I(\sigma_2),\ I(\sigma_{p-3}(2)).$$

For $\alpha = 1$, after choosing the constant $C_1 = -\frac{p+1}{2} + O(p^2)$ in theorem 27, where $O(p^2)$ is such that $\mathfrak{m}_0(C_1) = 0$, we have $v(\mathfrak{m}_w(C_1)) \geqslant 1$ for $w \in \{1,2,3,4\}$. There is the matrix

$$\begin{aligned}\mathfrak{M}'' &= \begin{pmatrix} \sum_{r-1>i(p-1)+1>1} \binom{r-1}{i(p-1)} & \sum_{r-1>i(p-1)+1>1} \binom{r}{i(p-1)+1} \\ \sum_{r-1>i(p-1)+1>1} \binom{r-1}{i(p-1)} i & \sum_{r-1>i(p-1)+1>1} \binom{r}{i(p-1)+1} i \end{pmatrix} \\ &\equiv_{p^2} \begin{pmatrix} 1-r+2p & 2-2r+2p \\ 3p(1-r) - \frac{(r-1)^2}{p-1} & 2p(1-r) - \frac{(r-1)(r-2)}{p-1} \end{pmatrix}.\end{aligned}$$

Then

$$\mathfrak{M}'' \begin{pmatrix} 1 \\ C_1 \end{pmatrix} = \mathfrak{M}'' \begin{pmatrix} 1 \\ -\frac{p+1}{2} \end{pmatrix} \equiv_{p^2} \begin{pmatrix} 0 \\ p - \frac{r}{2} \end{pmatrix}.$$

We consider two cases:

1. $r \not\equiv 2p \pmod{p^2(p-1)}$. Then theorem 27 applies, and we have that $\overline{\Theta}_{r+2,a}$ has a series

whose factors are quotients of submodules of

$$I\left(\sigma_2\right),\, I\left(\sigma_{p-3}(2)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$.

2. $r \equiv 2p \pmod{p^2(p-1)}$. In particular, since $r > 2p$, we have $r \geqslant p^2(p-1)+2p$. Then we have $v(\mathfrak{m}_w(C_1)) \geqslant 2$, where $\mathfrak{m}_w(C_1)$ is as in the statement of theorem 27. This is so since the expressions in $\mathfrak{m}_w(C_1)$ are equivalent modulo p^2 for any two weights which are congruent modulo $p^2(p-1)$, and the desired statement holds true when $r = 2p$. Moreover, $\binom{r-1}{0} - \frac{p+1}{2}\binom{r}{1} \equiv 1 - O(p) \equiv_p 1$, so theorem 27 applies, and we can conclude that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$\pi(0,0,\omega),\, I\left(\sigma_2\right),\, I\left(\sigma_{p-3}(2)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$.

— *The case when $s = 2$ and $r \equiv 1 \pmod{p}$.* By calling the methods `exceptional_cases(2,1,1)` and `gcd_for_the_matrix(2,1,1)`, we can show that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-1}(1)\right),\, I\left(\sigma_2\right),\, I\left(\sigma_{p-3}(2)\right).$$

Moreover, the output of `find_m_w(2,1,1)` shows that there are polynomials

$$\begin{aligned} f_1 &= \textstyle\sum_{r-1>i(p-1)+1>1} \Upsilon_i^{(1)} x^{i(p-1)+1} y^{r-i(p-1)-1}, \\ f_2 &= \textstyle\sum_{r-1>i(p-1)+1>1} \Upsilon_i^{(2)} x^{i(p-1)+1} y^{r-i(p-1)-1}, \end{aligned}$$

with integral coefficients, such that $[1, f_1]$ and $[1, f_2]$ are in the image of $T-a$, such that $\sum_{r-1>i(p-1)+1>1} \Upsilon_i^{(j)} = 0$, and such that $v(S_w^{(j)}) \geqslant 1$, where

$$S_w^{(j)} = \textstyle\sum_{r-1>i(p-1)+1>1} \Upsilon_i^{(j)} \binom{i}{w},$$

for all $w \in \{0,1,2,3,4\}$ and all $j \in \{1,2\}$. Moreover,

$$S_1^{(1)} \equiv S_1^{(2)} \equiv r - (p+1) \pmod{p^2}.$$

We consider two cases:

1. $r \not\equiv p+1 \pmod{p^2(p-1)}$. Then due to the proof of theorem 27 there is a polynomial

$$f' = \textstyle\sum_{r-1>i(p-1)+1>1} \Upsilon_i' x^{i(p-1)+1} y^{r-i(p-1)-1}$$

with integral coefficients, such that $[1, f'] + [1, \overline{\theta}^2 h'] + O(p^\delta)$ is in the image of $T-a$, for some h' and some $\delta > 0$, and such that

$$\begin{aligned} \textstyle\sum_{r-1>i(p-1)+1>1} \Upsilon_i' &= 1, \\ \textstyle\sum_{r-1>i(p-1)+1>1} i\Upsilon_i' &= -1. \end{aligned}$$

Then

$$\begin{aligned} f' + xy^{r-1} - 2x^{r-1}y &\in \ker \Psi_1 \subseteq \overline{\theta}\sigma_{r-(p+1)}, \\ f' + xy^{r-1} - 2x^{r-1}y &\notin \overline{\theta}^2 \sigma_{r-2(p+1)}, \end{aligned}$$

and hence $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_2\right), \, I\left(\sigma_{p-3}(2)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$.

2. $r \equiv p+1 \pmod{p^2(p-1)}$. In particular, since $r > p+1$, we have $r > p^2(p-1)+p$. Then, for any C_1 and any $w \in \{0,1,2,3,4\}$, we have $v(\mathfrak{m}_w(C_1)) \geqslant 2$, where $\mathfrak{m}_w(C_1)$ is as in the statement of theorem 27. This is so since the expressions in $\mathfrak{m}_w(C_1)$ are equivalent modulo p^2 for any two weights which are congruent modulo $p^2(p-1)$, and the desired statement holds true when $r = p+1$. Therefore, we can arbitrarily choose C_1 in a way that theorem 27 applies, and hence we can deduce that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$\pi(0,0,\omega), \, I\left(\sigma_2\right), \, I\left(\sigma_{p-3}(2)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$.

— *The case when $s=4$ and $r \not\equiv \{0,1,2,3,4\}$* $\pmod p$. Can be done in similar fashion as the case when $s=2$, or by calling the method `print_the_roots_for_all_matrices(2,True)` in the first program in the appendix.

— *The case when $s=4$ and $r \equiv 0$* $\pmod p$. In this case, only `find_m_w(2,0,2)` returns that the relevant $\mathfrak{m}_w(\varnothing)$ are divisible by r. The output of the method

`gcd_for_the_matrix(2,2,2)`

in the first program in the appendix shows that the factor in $\overline{\Theta}_{r+2,a}$ corresponding to $I\left(\sigma_0(2)\right)$ is trivial, since $\frac{1}{2}(r-1)(r-2)(r-3)(r-4) \neq 0$. Printing

`A.transpose().kernel().basis_matrix()`

in the method `exceptional_cases(2,2,2)` in the first program in the appendix shows that the factor in $\overline{\Theta}_{r+2,a}$ corresponding to $I\left(\sigma_{p-1}(2)\right)$ is trivial, since $\frac{1}{2}(r-2)(r-3) \neq 0$. These three facts together show that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$\pi(p-5,0,\omega^4), \, I\left(\sigma_{p-3}(3)\right), \, I\left(\sigma_2(1)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$, which completes this case of the proof.

— *The case when $s=4$ and $r \equiv \{1,2\}$* $\pmod p$. Since $2 > \alpha$, and since

$$\textstyle\sum_{i>0} \binom{r-1}{w}\binom{r-1-v}{i(p-1)} = O(p)$$

whenever $w > (r-1 \bmod p)$, the same calculations for $\mathfrak{m}_w(C_1)$ as in the case when $s \notin \{2,4\}$ and $t \equiv 1 \pmod p$ apply, showing that $\mathfrak{v}_1(C_1) = 1$. Similarly as in the proof of theorem 5, calling the method `find_m_w(2,alpha,2)` with `alpha` $= 0,1$ shows that in both cases the relevant $\mathfrak{m}_w(C_1,\ldots,C_\alpha)$ are polynomials which are divisible by $(r-1)(r-2)(r-3)$, which similarly completes this case of the proof.

— *The case when $s=4$ and $r \equiv 3$* $\pmod p$. From the output of the methods

`find_m_w(2,`α`,2)`, `exceptional_cases(2,1,2)`, `gcd_for_the_matrix(2,1,2)`,

with $\alpha = 0,1,2$, we get that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-3}(1)\right), \, I\left(\sigma_{p-1}(2)\right), \, \pi(0,0,\omega^2).$$

Note that $r > p+3$ implies that $r \geqslant p^2+3$, so we can follow the proof of theorem 27 to find an element in the kernel of reduction which gets mapped to $T[1,1]$ by Ψ_2, thus obtaining the $\pi(0,0,\omega^2)$ term. We consider two cases:

1. $r \not\equiv p+3 \pmod{p^2(p-1)}$. The output of the method `find_m_w(2,2,2)` shows that there are polynomials

$$
\begin{aligned}
f_1 &= \textstyle\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(1)} x^{i(p-1)+2} y^{r-i(p-1)-2},\\
f_2 &= \textstyle\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(2)} x^{i(p-1)+2} y^{r-i(p-1)-2},
\end{aligned}
$$

with integral coefficients, such that $[1,f_1]+O(p^{1+\delta})$ and $[1,f_2]+O(p^{1+\delta})$ are in the image of $T-a$, for some $\delta>0$, such that $\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(j)} = 0$, and such that $v(S_w^{(j)}) \geqslant 1$, where

$$S_w^{(j)} = \textstyle\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(j)} \binom{i}{w},$$

for all $w \in \{0,1,2,3\}$ and all $j \in \{1,2\}$. These two polynomials correspond to the last two columns of the output. In particular, $\Upsilon_i^{(1)} = \binom{r-1}{i(p-1)+1}$ and $\Upsilon_i^{(2)} = \binom{r}{i(p-1)+2}$. Let $\varkappa = \frac{r-(p+3)}{p}$, so that $v(\varkappa)=0$ by assumption. We can calculate, using lemma 21, that

$$\begin{pmatrix} S_0^{(1)} & S_0^{(2)} \\ S_1^{(1)} & S_1^{(2)} \\ S_2^{(1)} & S_2^{(2)} \end{pmatrix} \equiv_{p^2} \begin{pmatrix} -\frac{5}{2}\varkappa p & -5\varkappa p \\ -\frac{3}{2}\varkappa p & -\frac{5}{2}\varkappa p \\ \frac{1}{2}\varkappa p & \varkappa p \end{pmatrix}.$$

Consequently, from the proof of theorem 27 we can deduce that there are polynomials

$$
\begin{aligned}
f_1' &= \textstyle\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(1)'} x^{i(p-1)+2} y^{r-i(p-1)-2},\\
f_2' &= \textstyle\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(2)'} x^{i(p-1)+2} y^{r-i(p-1)-2},
\end{aligned}
$$

with integral coefficients, such that

$$
\begin{aligned}
&[1,f_1'] + [1,\overline{\theta}^3 h_1'] + O(p^\delta) \in \operatorname{im}(T-a),\\
&[1,f_2'] + [1,\overline{\theta}^3 h_2'] + O(p^\delta) \in \operatorname{im}(T-a),
\end{aligned}
$$

for some h_1', h_2' and some $\delta>0$, and such that

$$\begin{pmatrix} S_0^{(1)'} & S_0^{(2)'} \\ S_1^{(1)'} & S_1^{(2)'} \\ S_2^{(1)'} & S_2^{(2)'} \end{pmatrix} \equiv_p \begin{pmatrix} -5 & -10 \\ -3 & -5 \\ 1 & 2 \end{pmatrix},$$

where

$$S_w^{(j)'} = \textstyle\sum_{r-2>i(p-1)+2>2} \Upsilon_i^{(j)'} \binom{i}{w},$$

for all $w \in \{0,1,2,3\}$ and all $j \in \{1,2\}$. Note that

$$\begin{pmatrix} 1 \\ -1 \\ -2 \\ 1 \end{pmatrix} \in \ker \begin{pmatrix} 1 & 1 & -5 & -10 \\ 0 & 1 & -3 & -5 \\ -1 & -1 & 1 & 2 \end{pmatrix},$$

where the matrix is seen as a map of a vector space over $\mathbb{F}_p$, and hence

$$
\begin{aligned}
&x^2y^{r-2} - x^{r-2}y^2 - 2f_1' + f_2' \in \ker\Psi_1 \subseteq \overline{\theta}^2 \sigma_{r-2(p+1)},\\
&x^2y^{r-2} - x^{r-2}y^2 - 2f_1' + f_2' \notin \overline{\theta}^3 \sigma_{r-3(p+1)},
\end{aligned}
$$

(where $\overline{\theta}^3 \sigma_{r-3(p+1)}$ is the trivial subspace if $r < 3(p+1)$). Consequently, $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-3}(1)\right),\ \pi(0,0,\omega^2).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$.

2. $r \equiv p+3 \pmod{p^2(p-1)}$. In particular, since $r > p+3$, we have $r > p^2(p-1)+p$. For $\alpha = 1$, after choosing the constant $C_1 = -\frac{p}{3} + O(p^2)$ in theorem 27, where $O(p^2)$ is such that $\mathfrak{m}_0(C_1) = 0$, we have $v(\mathfrak{m}_w(C_1)) \geqslant 1$ for $w \in \{1,2,3,4\}$. There is the matrix

$$\begin{aligned}\mathfrak{M}'' &= \begin{pmatrix} \sum_{i>0} \binom{r-1}{i(p-1)} & \sum_{i>0} \binom{r}{i(p-1)+1} \\ \sum_{i>0} \binom{r-1}{i(p-1)} i & \sum_{i>0} \binom{r}{i(p-1)+1} i \end{pmatrix} \\ &\equiv_{p^2} \begin{pmatrix} \frac{p}{3} & \frac{11p}{6} + \frac{r-4}{p-1} \\ \frac{p(r-1)}{6} & \frac{p(11-2r)}{6} - \frac{r-4}{(p-1)^2} \end{pmatrix} \equiv_{p^2} \begin{pmatrix} \frac{p}{3} & \frac{11p}{6} + \frac{r-4}{p-1} \\ \frac{p}{3} & \frac{5p}{6} + \frac{4-r}{(p-1)^2} \end{pmatrix}.\end{aligned}$$

Then

$$\mathfrak{M}'' \binom{1}{C_1} = \mathfrak{M}'' \begin{pmatrix} 1 \\ -\frac{p}{3} \end{pmatrix} \equiv_{p^2} \binom{0}{0}.$$

Hence $v(\mathfrak{m}_1(C_1)) \geqslant 2$. Moreover, $v(\mathfrak{m}_w(C_1)) \geqslant 2$, for all $w \in \{2,3,4\}$, since that statement holds true for $r = p+3$. Consequently, theorem 27 applies, and we get that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$\pi(p-3,0,\omega),\ I\left(\sigma_{p-1}(2)\right),\ \pi(0,0,\omega^2).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$.

— *The case when $s = 4$ and $r \equiv 4 \pmod{p}$.* In this case, similarly as in the case when $s = 4$ and $r \equiv 0 \pmod{p}$, printing

```
A.transpose().kernel().basis_matrix()
```

in the method `exceptional_cases(2,2,2)` in the first program in the appendix shows that the factor in $\overline{\Theta}_{r+2,a}$ corresponding to $I\left(\sigma_{p-1}(2)\right)$ is trivial, since $\frac{1}{2}(r-2)(r-3) \neq 0$. Even though the output of the method

```
gcd_for_the_matrix(2,2,2)
```

in the first program in the appendix shows that the corresponding matrix does not have full rank, by printing that matrix we can see that its second row is equal to zero when $r \equiv 4 \pmod{p}$ and that $(0,0,1)^T$ is in its range. Consequently, the factor in $\overline{\Theta}_{r+2,a}$ corresponding to $I\left(\sigma_0(2)\right)$ must be trivial. The element $h = x^2y^{r-2} - y^2x^{r-2}$ is in the kernel of reduction, and

$$h = \overline{\theta}(a_1 xy^{r-p-2} + \cdots + a_{\lfloor r/(p-1) \rfloor} x^{r-p-2} y),$$

where

$$a_1 + \cdots + a_{\lfloor r/(p-1) \rfloor} \equiv_p 2 \not\equiv_p 0.$$

Consequently, $h \in \overline{\theta}\sigma_{r-(p+1)}$ and $h \notin \overline{\theta}^2\sigma_{r-2(p+1)}$, so there is a nontrivial element of $I_{r-2}(1)$ which is in the kernel of reduction. Since $I_{r-2}(1) \cong I_2(1)$ is not semi-simple, it follows from lemma 20 that the factor of $\overline{\Theta}_{r+2,a}$ which is a quotient of $I\left(\sigma_2(1)\right)$ must be trivial. These facts together show that $\overline{\Theta}_{r+2,a}$ has a series whose factors are quotients of submodules of

$$I\left(\sigma_{p-5}(4)\right),\ I\left(\sigma_{p-3}(3)\right).$$

These modules cannot pair up to give a reducible $\overline{\Theta}_{r+2,a}$, which completes this case of the proof.

— *The small leftover cases.* Since theorem 27 holds true under the assumption that $r > m(p+1)$, we are left with the cases when

$$(p,r) \in \{(3,6),(3,8),(5,12)\}.$$

The case when $(p,r) = (3,6)$ is trivial. For the case when $(p,r) = (3,8)$, note that

$$3xy^7 + 2\binom{7}{2}x^3y^5 + 2\binom{7}{4}x^5y^3 + 2\binom{7}{1}x^7y + E' = 3xy^7 + 42x^3y^5 + 70x^5y^3 + 14x^7y + E',$$

is in the image of $T - a$, where $v(E') \geqslant v(a) - 1 > 1$, and therefore $x^5y^3 - x^7y = \overline{\theta}x^4$ is in the kernel of reduction. Similarly, $xy^7 - x^3y^5$ is in the kernel of reduction, and we know that xy^7, x^7y are in the kernel of reduction, so $x^3y^5 - x^5y^3 = \overline{\theta}x^2y^2$ is in the kernel of reduction as well. In particular, $\overline{\Theta}_{10,a}$ must be $\pi(0,0,1)$. For the case when $(p,r) = (5,12)$, note that

$$5xy^{11} + 4\binom{11}{4}x^5y^7 + 4\binom{11}{8}x^9y^3 + E'' = 5xy^{11} + 1320x^5y^7 + 660x^9y^3 + E''$$

is in the image of $T - a$, where $v(E'') \geqslant v(a) - 1 > 1$, and therefore

$$xy^{11} + 264x^5y^7 + 132x^9y^3 + E'''$$

is in the image of $T - a$, where $v(E''') \geqslant v(a) - 2 > 0$. Since we know that xy^{11} is in the kernel of reduction, it follows that $-xy^{11} - x^5y^7 + 2x^9y^3 = \overline{\theta}(4y^6 + 3x^4y^2)$ is in the kernel of reduction. Similarly,

$$5y^{12} + 4\binom{11}{3}x^4y^8 + 4\binom{11}{7}x^8y^4 + 4\binom{11}{11}x^{12} + E''''$$

is in the image of $T - a$, where $v(E'''') \geqslant v(a) - 1 > 1$. Moreover, $x^{12} + O(p^2)$ is in the image of $T - a$. Consequently, $y^{12} + 2x^4y^8 - x^8y^4$ is in the kernel of reduction. In particular, $\overline{\Theta}_{14,a}$ must be $\pi(2,0,\omega)$.

□

5.3 The case when $6 > v(a) > 3$

In this subsection, we will complete the proof of theorem 7, and we will also prove the first and the third part of theorem 9.

Proof of theorem 7. The case when $p = 3$ is vacuous, so in the remainder of this proof we are going to assume that $p > 3$.

— *The case when $s \notin \{2,4,6\}$ and consequently $t \not\equiv \{0,1,2\}$* (mod p). The proof of this case is similar to the first case in the proof of theorem 6. The program written in `Sage` listed in the appendix completely automates this proof. More specifically, for each $0 \leqslant \alpha < m$, it finds constants $C_1, \ldots, C_\alpha$ such that $v(C_i) \geqslant 1$, for all $1 \leqslant i \leqslant \alpha$, and $\mathfrak{m}_w(C_1, \ldots, C_\alpha) = 0$, for all $0 \leqslant w < \alpha$. Then, it calculates that $\mathfrak{m}_\alpha(C_1, \ldots, C_\alpha) \not\equiv 0 \pmod{p^2}$, which holds true due to the fact that $t \not\equiv \{0,1,2\} \pmod{p}$. Since $\mathfrak{m}_w(C_1, \ldots, C_\alpha)$ is a linear combination of sums of the type $\sum_{j(p-1)>0} \binom{r-\alpha-v}{j(p-1)}$, for $0 \leqslant v \leqslant w$, and each of these sums has positive valuation since $s - \alpha - w \geqslant s - \alpha - (2m + 1 - \alpha) > 0$, it follows that $v(\mathfrak{m}_w(C_1, \ldots, C_\alpha)) \geqslant 1$, for all $\alpha < w \leqslant 2m + 1 - \alpha$. Thus, theorem 27 applies, and it implies that $\overline{\Theta}_{r+2,a}$ must in fact be isomorphic to $\pi(s - 2m, 0, \omega^m)$, which is irreducible.

— *The case when $s \in \{2,4,6\}$.* Can be done in similar fashion as the case when $s = 2$ in the proof of theorem 6, or by calling the method `print_the_roots_for_all_matrices(3,True)` in the first program in the appendix, and the remaining cases being dealt with as in the proof of theorem 6.

□

The above proof follows the same outline as the proof of theorem 6, and it can be completely automated. The method `verify_conjecture_eight(m)`, with $\mathtt{m} = x$, combines the two cases in

the proof and simply prints whether conjecture 8 is true for $m = x$.

Proof of the first part of theorem 9. Can be done in similar fashion as the proof of theorem 6, or by calling the method `verify_conjecture_eight(m)` in the first program in the appendix, for each $4 \leqslant m < 6$. □

Proof of the third part of theorem 9. Follows from theorem 6. □

5.4 The general case

In this subsection, we will complete the proof of the second part of theorem 9.

Proof of the second part of theorem 9. The proof of this case follows the same outline as the first case in the proof of theorem 6. Let m be the integer such that $m+1 > v(a) > m$. In this case, $s \notin \{2, \ldots, 2m\}$, which implies that $p > 2m+1$. Suppose that, for each $\alpha \in \{0, \ldots, m-1\}$, we find terms $C_1, \ldots, C_\alpha$ such that $v(\mathfrak{m}_\alpha(C_1, \ldots, C_\alpha)) = 1$. It can be proven as in the proof of theorem 7 that $v(\mathfrak{m}_w(C_1, \ldots, C_\alpha)) \geqslant 1$, for all $\alpha < w \leqslant 2m+1-\alpha$. Therefore, supposing we find suitable terms $C_1, \ldots, C_\alpha$, theorem 27 will apply, and it will imply that $\overline{\Theta}_{r+2,a}$ must in fact be isomorphic to $\pi(s-2m, 0, \omega^m)$. Consequently, the proof of the second part of theorem 9 will be completed once we show the existence of suitable terms $C_1, \ldots, C_\alpha$. In fact, for each $1 \leqslant j \leqslant \alpha$, we will explicitly define C_j by $C_j = pc_j$, where

$$c_j = j!\tbinom{\alpha}{j}\tfrac{(-1)^j(s+1-r)}{(s-2\alpha+1+j)\cdots(s-2\alpha+1)} + j!\tbinom{\alpha+1}{j+1}\tfrac{(-1)^j(r-\alpha)}{(s-2\alpha+1+j)\cdots(s-2\alpha+1)} + O(p).$$

In order to show that $C_1, \ldots, C_\alpha$ satisfy the desired properties, we must show that

$$A(1, C_1, \ldots, C_\alpha)^T = (0, \ldots, 0, pu)^T,$$

where $u \in \mathbb{Z}_p$ is a unit, and A is a $(\alpha+1) \times (\alpha+1)$ matrix defined by

$$\begin{aligned} A_{w,0} &= p\tfrac{(-1)^w(s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}} + O(p^2), \\ A_{w,j} &= \textstyle\sum_v (-1)^{w-v}\tbinom{j+w-v-1}{w-v}\tbinom{r-\alpha+j}{v}\left(\tbinom{s-\alpha+j-v}{j-v} - \tbinom{r-\alpha+j-v}{j-v}\right) + O(p), \end{aligned}$$

where we index the entries by $w \in \{0, \ldots, \alpha\}$ and $j \in \{1, \ldots, \alpha\}$. Equivalently, we want to show that

$$B(1, c_1, \ldots, c_\alpha)^T = (0, \ldots, 0, u)^T,$$

where $u \in \mathbb{Z}_p$ is a unit, and B is a $(\alpha+1) \times (\alpha+1)$ matrix defined by

$$\begin{aligned} B_{w,0} &= \tfrac{(-1)^w(s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}} + O(p), \\ B_{w,j} &= \textstyle\sum_v (-1)^{w-v}\tbinom{j+w-v-1}{w-v}\tbinom{r-\alpha+j}{v}\left(\tbinom{s-\alpha+j-v}{j-v} - \tbinom{r-\alpha+j-v}{j-v}\right) + O(p). \end{aligned}$$

We will slightly abuse notation and view $c_1, \ldots, c_\alpha, B, u$ as being reduced modulo p, thus dropping the $O(p)$ terms. We will prove that $B(1, c_1, \ldots, c_\alpha)^T = (0, \ldots, 0, u)^T$, where $u = \frac{(s-r)_{\alpha+1}}{(s-\alpha)_{\alpha+1}}$. First, note that

$$\textstyle\sum_{w\geqslant 0} X^w \sum_v (-1)^{w-v}\tbinom{j+w-v-1}{w-v}\tbinom{j}{v} = \sum_v (-X)^v (1-X)^{-j}\tbinom{j}{v} = (1-X)^j(1-X)^{-j} = 1,$$

so $\sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{j}{v} = \delta_{w=0}$. Therefore,

$$\begin{aligned}\sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{r-\alpha+j}{v} \binom{r-\alpha+j-v}{j-v} &= \binom{r-\alpha+j}{j} \sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{j}{v} \\ &= \delta_{w=0} \binom{r-\alpha+j}{j}.\end{aligned}$$

Consequently, the matrix B is given by

$$\begin{aligned}B_{w,0} &= \tfrac{(-1)^w (s-r)(r-\alpha)_w}{(s-\alpha)_{w+1}} + O(p), \\ B_{w,j} &= -\delta_{w=0} \binom{r-\alpha+j}{j} + \sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{r-\alpha+j}{v} \binom{s-\alpha+j-v}{j-v} + O(p).\end{aligned}$$

We are going to consider two cases, when $w = 0$ and when $w > 0$.

— *The case when* $w = 0$. In this case, we want to show that

$$\sum_{j=1}^{\alpha} c_j \left(\binom{s-\alpha+j}{j} - \binom{r-\alpha+j}{j} \right) = \delta_{\alpha \neq 0} \tfrac{r-s}{s-\alpha},$$

reduced modulo p. If $\alpha = 0$, then the left side is the empty sum, so the identity is vacuously true. Suppose that $\alpha > 0$. We are going to view the terms in the identity as rational functions in the formal variables r and s, over the field $\mathbb{Q}$. Then we can replace r and s by $r + \alpha$ and $s + \alpha$, which leaves us with the task of showing the identity

$$\Xi(r, s) := \sum_j \tfrac{(-1)^j j!}{j+1} \binom{\alpha}{j} \tfrac{(j+1)(s+1)+(\alpha-j)r}{(s-\alpha+1+j)\cdots(s-\alpha+1)} \left(\binom{s+j}{j} - \binom{r+j}{j} \right) = \tfrac{r-s}{s}.$$

Note that

$$\begin{aligned}\Xi(r+1, s) - \Xi(r, s) &= \sum_j \tfrac{(-1)^j j!}{j+1} \binom{\alpha}{j} \tfrac{\alpha-j}{(s-\alpha+1+j)\cdots(s-\alpha+1)} \binom{s+j}{j} \\ &\quad - \sum_j (-1)^j j! \binom{\alpha}{j} \tfrac{s+1-\alpha+j}{(s-\alpha+1+j)\cdots(s-\alpha+1)} \binom{r+j}{j-1} \\ &\quad - \sum_j (-1)^j j! \binom{\alpha}{j} \tfrac{\alpha-j}{(s-\alpha+1+j)\cdots(s-\alpha+1)} \binom{r+j+1}{j} \\ &= \sum_j \tfrac{(-1)^j j!}{j+1} \binom{\alpha}{j} \tfrac{\alpha-j}{(s-\alpha+1+j)\cdots(s-\alpha+1)} \binom{s+j}{j} \\ &\quad - \sum_j (-1)^j j! \binom{\alpha}{j} \tfrac{1}{(s-\alpha+j)\cdots(s-\alpha+1)} \binom{r+j}{j-1} \\ &\quad - \sum_j (-1)^{j-1} (j-1)! \binom{\alpha}{j-1} \tfrac{\alpha-j+1}{(s-\alpha+j)\cdots(s-\alpha+1)} \binom{r+j}{j-1} \\ &= \sum_j \tfrac{(-1)^j j!}{j+1} \binom{\alpha}{j} \tfrac{\alpha-j}{(s-\alpha+1+j)\cdots(s-\alpha+1)} \binom{s+j}{j} \\ &\quad + \sum_j \tfrac{(-1)^j (j-1)!}{(s-\alpha+j)\cdots(s-\alpha+1)} \binom{r+j}{j-1} \left((\alpha-j+1) \binom{\alpha}{j-1} - j \binom{\alpha}{j} \right) \\ &= \sum_{j \geqslant 0} \binom{\alpha}{j+1} \binom{s+j}{j} \tfrac{(-1)^j j!}{(s-\alpha+1+j)\cdots(s-\alpha+1)} = g(s),\end{aligned}$$

since $(\alpha - j + 1)\binom{\alpha}{j-1} = j\binom{\alpha}{j}$. In particular, since $\Xi(r, s)$ is a polynomial in r, it follows that $\Xi(r, s)$ must be linear in r. By combining this fact with the fact that $\Xi(s, s) = 0$, we get that $\Xi(r, s) = (r - s)g(s)$. This leaves us with the task of showing the identity

$$sg(s) = \sum_{j \geqslant 0} (-1)^j \binom{\alpha}{j+1} \tfrac{(s+j)_{j+1}}{(s-\alpha+1+j)_{j+1}} = 1,$$

which is equivalent to

$$h(\alpha, s) = 1 - sg(s) = -\sum_j (-1)^j \binom{\alpha}{j+1} \tfrac{(s+j)_{j+1}}{(s-\alpha+1+j)_{j+1}} = \sum_j (-1)^j \binom{\alpha}{j} \tfrac{(s-1+j)_j}{(s-\alpha+j)_j} = 0.$$

Note that $h(\alpha, s) = {}_2F_1(-a, s; -a + s + 1; 1)$ can be written explicitly in closed form by using Euler's formula

$${}_2F_1(a, b; c; z) = \tfrac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 \tfrac{t^{b-1}(1-t)^{c-b-1}}{(1-tz)^a} \, \mathrm{d}t,$$

which is given in [2]. Specifically, $h(\alpha, s) = {}_2F_1(-a, s; -a+s+1; 1) = \frac{\Gamma(-a+s+1)}{\Gamma(s+1)\Gamma(1-a)} = 0$, as $\Gamma(1-a) = \infty$, and $\Gamma(-a+s+1)$ and $\Gamma(s+1)$ are finite.

— *The case when* $w \neq 0$. In this case, we want to show that

$$\sum_{j=1}^{\alpha} c_j \sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{r-\alpha+j}{v} \binom{s-\alpha+j-v}{j-v} = \frac{(-1)^w (r-s)(r-\alpha)_w}{(s-\alpha)_{w+1}} + \delta_{w=\alpha} \frac{(s-r)_{\alpha+1}}{(s-\alpha)_{\alpha+1}},$$

for all $0 < w \leqslant \alpha$. Suppose that $\alpha > 0$. Again, we are going to view the terms in the identity as rational functions in the formal variables r and s, over the field $\mathbb{Q}$. Then we can replace r and s by $r+\alpha$ and $s+\alpha$, which leaves us with the task of showing the identity

$$\Xi_w(r,s) := \sum_{j=1}^{\alpha} d_j \sum_v (-1)^{w-v} \binom{j+w-v-1}{w-v} \binom{r+j}{v} \binom{s+j-v}{j-v} = \frac{(-1)^w (r-s)(r)_w}{(s)_{w+1}} + \delta_{w=\alpha} \frac{(s-r)_{\alpha+1}}{(s)_{\alpha+1}},$$

where

$$d_j = \frac{(-1)^j j!}{j+1} \binom{\alpha}{j} \frac{(j+1)(s+1)+(\alpha-j)r}{(s-\alpha+1+j)\cdots(s-\alpha+1)}.$$

This identity can be verified by a computer for all $\alpha \leqslant 36$, which completes the proof of the second part of theorem 9.

□

A Appendix

A.1 Calculations with Sage

A.1.1 Verifying conjecture 8

The following program can be used to find the determinants of the relevant square submatrices of $\mathfrak{M}^{(r,m,\alpha)}$, find their greatest common divisor as a polynomial in r, and list a basis for the kernel of the matrix $\mathfrak{M}^{(r,m,\alpha)}$ seen as a linear operator over $\mathbb{F}_p$. In particular, calling the method `print_the_roots_for_all_matrices(m,True)` with $\mathtt{m} = x$ lists the possible congruence classes modulo p outside of which $\overline{\Theta}_{r+2,a}$ is irreducible, for $m = x$ and for each possible $s \in \{2, \ldots, 2x\}$. The method `verify_conjecture_eight(m)`, with $\mathtt{m} = x$, combines this with theorem 27, as explained in subsection 5.3, and simply prints whether the first two parts of conjecture 8 are true for $m = x$.

conjecture_eight.sage

```
from operator import mul
[r,s,t,p,v] = var('r s t p v')
Ring = FractionField(PolynomialRing(QQ,['r','s','t','p']))

def factorise(g):
    return g.factor() if g!=0 else g

# Returns the roots of g as a sorted list.
def get_roots(g):
    if g!=0:
        list_of_roots = g.roots()
        for i in range(0,len(list_of_roots)):
            list_of_roots[i] = list_of_roots[i][0]
        list_of_roots.sort()
        return list_of_roots
    return []

```

```
# Returns $\eta(X,Y)$, from lemma 25.
def eta(X,Y):
    if X>=1 and Y>=0:
        return binomial(X,Y)
    if X<1 and Y>=0:
        return 2*binomial(X-1,Y) if X==0 and Y==0 else binomial(X-1,Y)
    if X<1 and Y<0:
        return binomial(X-1,X-Y) if X>=Y else 0
    return 0

# Returns the matrix $A$ with $r$ substituted by $e$.
def substitute_in_matrix(A,e):
    B = copy(A)
    for i in range(0,B.nrows()):
        for j in range(0,B.ncols()):
            B[i,j]= A[i,j].subs(r=e)
    return B

# Returns the matrix $\mathfrak{M}^{(r,m,\alpha)}$, from lemma 26.
def construct_matrix(m,alpha,L):
    # $M$ is the number of rows, $N+2$ is the number of columns.
    M = alpha+1; N = m+1; A = matrix(Ring,M,N+2)

    # Filling in the first two columns.
    A[0,0] = 1; A[M-1,0] = A[M-1,0]-(-1)^(alpha)
    if L>=alpha and m+alpha>=2*L:
        for w in range(0,M):
            A[w,1] = binomial(2*L-r,w)
        A[M-1,1] = A[M-1,1]-1

    # Filling in the last $N$ columns.
    for l in range(alpha-m,M):
        for w in range(0,M):
            a = -binomial(r-alpha+l,2*L-alpha)*binomial(2*L-r,w) if m+alpha>=2*L else 0
            b = -binomial(r-alpha+l,l)*binomial(0,w) \
                    +sum([(-1)^(v)*binomial(l-v,w-v)*eta(2*L-alpha+l-v,l-v) \
                        *binomial(r-alpha+l,v) for v in range(0,w+1)])
            A[w,l+2-alpha+m] = factorise(simplify(a+b))
    return A

# Returns the relevant matrix arising from theorem 27, when $s > 2m$.
def construct_big_matrix(m,alpha):
    # $M$ is the number of rows and the number of columns.
    M = alpha+1; A = matrix(Ring,M,M)

    for l in range(0,M):
        for w in range(0,M):
            a = (s-r)*(p/(s-alpha))*(binomial(r-alpha,w)/binomial(s-alpha-1,w)) if l==0 else 0
            b = -binomial(r-alpha+l,l)*binomial(0,w) \
                    +sum([(-1)^(w-v)*binomial(l+w-v-1,w-v)*binomial(s-alpha+l-v,l-v) \
                        *binomial(r-alpha+l,v) for v in range(0,w+1)])
            A[w,l] = factorise(simplify(a*(-1)^w+b))
    return A

# Returns a polynomial whose roots are exceptional congruence
# classes of $r$ modulo $p$ outside of which the relevant factors of
# $\overline{\theta}^{\alpha}\sigma_{r-\alpha(p+1)}/\overline{\theta}^{\alpha+1}\sigma_{r-(\alpha+1)(p+1)}$ cancel, as can be shown by lemma 18.
def exceptional_cases(m,alpha,L):
    A = construct_matrix(m,alpha,L); product = 1
    product *= A[0,0]*A.transpose().kernel().basis_matrix()[0,0]
    if A.transpose().kernel().basis_matrix()[0,m+2] != 0:
        product /= A.transpose().kernel().basis_matrix()[0,m+2]
    if 2*L-1>=alpha and alpha>=L:
        product *= gcd_for_the_matrix(m,alpha,L)
    return product

# Returns the greatest common divisor of the determinants of the relevant
```

```
# square submatrices of $\mathfrak{M}^{(r,m,\alpha)}$, seen as polynomials in $r$ over $\mathbb{Q}$.
def gcd_for_the_matrix(m,alpha,L):
    # $M$ is the number of rows, $N+2$ is the number of columns.
    M = alpha+1; N = m+1; A = construct_matrix(m,alpha,L)
    B = A.matrix_from_rows_and_columns(range(0,M), range(0,2)+range(N-M+2,N+2))
    f = range(0,binomial(M+2,M)); counter = 0
    for i in range(0,M+2):
        for j in range (i+1,M+2):
            entries = range(0,M+2); entries.remove(i); entries.remove(j)
            f[counter] = B.matrix_from_rows_and_columns(range(0,M), entries).det()
            counter += 1
    return gcd(f)

# Returns a polynomial whose roots are exceptional congruence
# classes of $r$ modulo $p$ outside of which the relevant factors of
# $\overline{\theta}^{\alpha}\sigma_{r-\alpha(p+1)}/\overline{\theta}^{\alpha+1}\sigma_{r-(\alpha+1)(p+1)}$ cancel, in the case $s \notin \{2,\ldots,2m\}$.
def polynomial_from_the_big_matrix(m,alpha):
    # $M$ is the number of rows and the number of columns.
    M = alpha+1; A = construct_big_matrix(m,alpha)
    for i in range(0,M):
        A[i,0] = A[i,0]/p
    B = A.matrix_from_rows_and_columns(range(0,M-1), range(0,M))
    C = B.transpose().kernel().basis_matrix()
    x = sum([A[M-1,v]*C[0,v] for v in range(0,M)])
    return x.subs(r=s-t) if C[0,0]==1 else (t+1)

# Returns the product of all polynomials for all choices for $\alpha$.
def the_roots_for_all_big_matrices(m):
    return reduce(mul,[polynomial_from_the_big_matrix(m,alpha) \
                    for alpha in range(0,m)],1)

def print_the_gcd_for_the_matrix(m,alpha,L):
    A = construct_matrix(m,alpha,L)
    g = gcd_for_the_matrix(m,alpha,L)
    print A
    if g!=0:
        if g.roots()!=[]:
            for zeta in g.roots():
                print "Substituting r=%d in the matrix,"%zeta[0], \
                    "with m=%d, L=%d, alpha=%d, yields"%(m, L, alpha)
                print substitute_in_matrix(A,zeta[0])
    print A.transpose().kernel()
    print "For m=%d, L=%d, alpha=%d, the GCD of the determinants ="%(m, L, alpha), \
                factorise(g), "\n\n"

def print_the_roots_for_all_matrices(m,quiet):
    for L in range(1,m+1):
        product = r/r
        for alpha in range(1,m+1):
            product = product*exceptional_cases(m,alpha,L)
            if quiet==False:
                print_the_gcd_for_the_matrix(m,alpha,L)
        print "In the case when m=%d and s=%d, Theta^bar is irreducible unless"%(m, 2*L), \
                "r is congruent to one of the following numbers modulo p:"
        print get_roots(product), "\n\n\n\n"

# Returns a list of exceptional congruence classes of $r$
# modulo $p$ outside of which $\overline{\Theta}_{r+2,a}$ is irreducible.
def print_everything(m):
    print_the_roots_for_all_matrices(m,True)
    print "In the case when m=%d and s=/=2,...,%d, Theta^bar is irreducible unless"%(m, 2*m), \
                "the following polynomial vanishes modulo p, with t=s-r:"
    print the_roots_for_all_big_matrices(m)

def verify_conjecture_eight(m):
    conjecture_is_true = True
    for L in range(1,m+1):
```

```
        product = r/r
        for alpha in range(1,m+1):
            product = product*exceptional_cases(m,alpha,L)
        roots = get_roots(product)
        if min(roots)<2*(L-m) or max(roots)>2*L:
            conjecture_is_true = False
    f = the_roots_for_all_big_matrices(m)
    g = reduce(mul,[(t-alpha)^m for alpha in range(0,m)],1)
    if Ring(g/f).factor().is_integral()==False:
        conjecture_is_true = False
    if conjecture_is_true==True:
        print "When m=%d, the first two parts of conjecture eight are true."%m
    if conjecture_is_true==False:
        print "When m=%d, the first two parts of conjecture eight are not necessarily true!"%m
```

A.1.2 Finding $\mathfrak{m}_w(C_1, \dots, C_\alpha)$

The following program can be used to find suitable constants $C_1, \dots, C_\alpha$ as in the statement of theorem 27, and calculate the expressions $\mathfrak{m}_w$, for $0 \leqslant w \leqslant 2m+1-\alpha$. In particular, calling the method `find_m_w(m,alpha,L)` with `m` $= m$, and `alpha` $= \alpha$, and `L` $= L$, lists

$$\mathfrak{m}_0(C_1, \dots, C_\alpha), \dots, \mathfrak{m}_{2m+1-\alpha}(C_1, \dots, C_\alpha).$$

m_w.sage

```
[r,s,t,p,v] = var('r s t p v')
Ring = FractionField(PolynomialRing(QQ,['r','s','t','p']))

def factorise(g):
    return g.factor() if g!=0 else g

# Returns η(X,Y), from lemma 25.
def eta(X,Y):
    if X>=1 and Y>=0:
        return binomial(X,Y)
    if X<1 and Y>=0:
        return 2*binomial(X-1,Y) if X==0 and Y==0 else binomial(X-1,Y)
    if X<1 and Y<0:
        return binomial(X-1,X-Y) if X>=Y else 0
    return 0

# Returns the relevant matrix mod p arising from theorem 27, when s < 2m.
def construct_small_matrix(m,alpha,L):
    # N is the number of rows, M is the number of columns.
    M = alpha+1; N = 2*m+2-alpha; A = matrix(Ring,N,M)

    for l in range(0,M):
        for w in range(0,N):
            a = -binomial(r-alpha+l,2*L-alpha)*binomial(2*L-r,w) if alpha>=L else 0
            b = -binomial(r-alpha+l,l)*binomial(0,w) \
                    +sum([(-1)^(v)*binomial(l-v,w-v)*eta(2*L-alpha+l-v,l-v) \
                        *binomial(r-alpha+l,v) for v in range(0,w+1)])
            A[w,l] = factorise(simplify(a+b))
    return A

# Returns the list [m_0,...,m_{2m+1-α}].
def find_m_w(m,alpha,L):
    # N is the number of rows, M is the number of columns.
    M = alpha+1; N = 2*m+2-alpha; A = construct_small_matrix(m,alpha,L)
    B = A.matrix_from_rows_and_columns(range(0,M-1), range(0,M))
    C = B.transpose().kernel().basis_matrix()
    print "The list of constants C_l is", C
```

```
    x = range(0,N)
    for j in range(0,N):
        x[j] = factorise(sum([A[j,v]*C[0,v] for v in range(0,M)]))
    return x
```

Acknowledgments

I would like to thank my advisor, Professor Kevin Buzzard, for his helpful remarks, suggestions, and support. This work was supported by Imperial College London.

References

[1] Avner Ash and Glenn Stevens, *Modular forms in characteristic ℓ and special values of their L-functions,* Duke Mathematical Journal, **53** (1986), #3, 849–868.

[2] Wilfrid Norman Bailey, *Generalized Hypergeometric Series,* Cambridge Tracts in Mathematics and Mathematical Physics, Cambridge University Press **32** (1935), 4–5.

[3] Laurent Berger, *Représentations modulaires de $\mathrm{GL}_2(\mathbb{Q}_p)$ et représentations galoisiennes de dimension 2,* Astérisque **330** (2010) 263–279.

[4] ———, *La correspondance de Langlands locale p-adique pour $\mathrm{GL}_2(\mathbb{Q}_p)$,* Astérisque **339** (2011) 157–180.

[5] ———, *Local constancy for the reduction $\bmod p$ of two-dimensional crystalline representations,* Bulletin of the London Mathematical Society **44** (2012), #3, 451–459.

[6] Laurent Berger and Christophe Breuil, *Sur quelques représentations potentiellement cristallines de $\mathrm{GL}_2(\mathbb{Q}_p)$,* Astérisque **330** (2010) 155–211.

[7] Laurent Berger, Hanfeng Li, and Hui June Zhu, *Construction of some families of two-dimensional crystalline representations,* Mathematische Annalen **329** (2004), #2, 365–377.

[8] Christophe Breuil, *Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbb{Q}_p)$, I,* Compositio Mathematica **138** (2003), #2, 165–188.

[9] ———, *Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbb{Q}_p)$, II,* Journal of the Institute of Mathematics of Jussieu **2** (2003), #1, 23–58.

[10] ———, *Remarks on some locally $\mathbb{Q}_p$-analytic representations of $\mathrm{GL}_2(F)$ in the crystalline case,* London Mathematical Society Lecture Note Series **393** (2012), 212–238.

[11] Christophe Breuil and Ariane Mézard, *Multiplicités modulaires et représentations de $\mathrm{GL}_2(\mathbb{Z}_p)$ et de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ en $\ell = p$,* Duke Mathematical Journal **115** (2002), #2, 205–310.

[12] Christophe Breuil and Matthew Emerton, *Représentations p-adiques ordinaires de $\mathrm{GL}_2(\mathbb{Q}_p)$ et compatibilité local-global,* Astérisque **331** (2010), 255–315.

[13] Kevin Buzzard, *Questions about slopes of modular forms,* Astérisque **298** (2005), 1–15.

[14] Kevin Buzzard and Toby Gee, *Explicit reduction modulo p of certain two-dimensional crystalline representations,* International Mathematics Research Notices (2009), #12, 2303–2317.

[15] ———, *Explicit reduction modulo p of certain two-dimensional crystalline Galois representations, II,* Bulletin of the London Mathematical Society **45** (2013), #4, 779–788.

[16] ———, *Slopes of modular forms,* preprint (2015).

[17] Kevin Buzzard and Lloyd James Peter Kilford, *The 2-adic eigencurve at the boundary of weight space,* Compositio Mathematica, **141** (2005), #3, 605–619.

[18] Toby Gee, *Automorphic lifts of prescribed types,* Mathematische Annalen, **350** (2011), #1, 107–144.

[19] Lloyd James Peter Kilford, *On the slopes of the U_5 operator acting on overconvergent modular forms,* Journal de Théorie des Nombres de Bordeaux, **29** (2008), #1, 165–182.

[20] Lloyd James Peter Kilford and Ken McMurdy, *Slopes of the U_7 operator acting on a space of overconvergent modular forms,* LMS Journal of Computation and Mathematics, **15** (2012), 113–139.

[21] Ruochuan Liu, Daqing Wan, and Liang Xiao, *Eigencurve over the boundary of the weight space,* preprint (2014).

[22] David Roe, *The 3-adic eigencurve at the boundary of weight space,* International Journal of Number Theory, **10** (2014), #7, 1791–1806.

[23] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids 1*, Annales Scientifiques de l'École Normale Supérieure, **7** (1974), #4, 507–530.

[24] Daqing Wan, Liang Xiao, and Jun Zhang, *Slopes of eigencurves over boundary disks,* preprint (2014).

[25] Andrew Wiles, *On ordinary λ-adic representations associated to modular forms*, Inventiones mathematicae, **94** (1988), #3, 529–573.